Usable Secure Interfaces for Mobile Devices

Thesis submitted in accordance with the requirements of the University of Liverpool for the degree of Doctor in Philosophy by

ILESANMI AYODEJI OLADE

July 20, 2020

Abstract

The aim of this thesis is to address and contribute to the research evidence on what it means to implement usable security interfaces in mobile devices given their increasing importance in our daily lives. We focused on user interfaces for authentication while incorporating HCI principles to develop and explore design and usability issues. We have done so by directly observing and reporting on our three different works, with special attention given to the user practices that create security lapses and usability drawbacks.

The novelty of this research is the confirmation of the integral relationship across our three works showing that understanding and exploiting inherent human-factors such as memorability, tactile attributes, kinesiology and other inherent properties for human computer interface (HCI) designs improves security, usability and acceptance. One of our tasks is re-conceptualizing mobile device interfaces to make them both secure and usable. Our research indicates that interfaces that combine tactile and behavioural human characteristics into their basic design paradigm are more usable, and systems based on core graphical tokens with mnemonic properties result in higher memorability and familiarity values, while error recovery is strongly influenced by system design. Therefore system interfaces that can accommodate other familiar compound activities by users greatly reduce errors. One of our works proposes a new graphical authentication prototype interface to evaluate our research questions empirically. Our findings indicated that our first work, SemanticLock, had superior performance on key metrics such as password entry speed, memorability, encumbrance, user acceptance, usability, and likeability when compared with the PATTERN and PIN authentication techniques.

Secondly, we explored the acceptable levels of complexity an interface could have in order to be secure and yet still usable by shifting the focus of our second work to the popular virtual reality device (VR) ecosystem. This work involved immersing participants in a virtual reality environment where they created passwords on virtual reality versions

of popular mobile device authentication systems with different virtual reality interaction methods. The virtual reality system allowed us to evaluate the interface and interaction challenges by providing numerous heterogeneous interaction methods. We explored the outcome of porting the popular PATTERN authentication system into the virtual reality environment. We used the mobile device version of PATTERN as a control and the report indicates that PATTERN in VR is moderately fast, functionally usable and highly resistant to shoulder-surfing.

For our third work, we examined various technological impediments that make it difficult to develop secure interfaces and proposed alternatives such as transparent interfaces that rely solely on the user‘s biometric signatures. We explored this challenge with a virtual reality (VR) based prototype based on kinesiology, effectively capturing the biometric movement of the participants in VR, and collecting the discerning identifying factors from each person via machine-learning assisted processes. We evaluated large datasets of head, eyes and hand movements using machine learning to create a continuous transparent biometric authentication system. We attained a classification accuracy of 99.7% and determined that kinesiologically replicating a valid participant with false-positive data is extremely difficult, thus making this system highly secure and usable.

Our three major works conceptually explore the significant effects of user interactions on the effective security of their mobile devices. In our first study we determined various baselines in HCI that were used across the other works. The second work examined the practical effect of different interaction modes, while the third work explored using the interactions itself as a resultant effect of security. The compounding relevance among the works is the user.

Acknowledgements

This work is supported by the Department of Computer Science, University of Liverpool and the Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University.

It has been a tremendous privilege to carry out this research surrounded by very supportive colleagues, supervisors, and advisors at the University of Liverpool, UK, and Xi'an Jiaotong-Liverpool University, China.

My most profound acknowledgment goes to my Supervisors Dr. Hai-Ning Liang and Dr. Charles Fleming, for their meticulous guidance, research ideas, and feedback. This gratitude also extends to my co-supervisors, Dr. Xin Huang and Dr. Terry Payne for their immeasurable advice and support throughout my PhD studies. I am forever grateful to Ms. Tonie Jonna Poole aka "Aunty J" for all her efforts in proof-reading and correcting grammatical errors in my thesis.

Finally, I am grateful to my Mother, close friends and family from Nigeria and all around the world for every bit of support and encouragement I received; my journey was smoother because of you.

Contents

List of Abbreviations

ANOVA Analysis of variance. 50

CCP Cue Click Points. 14

CGP Cued Gazed ClickPoint. 14

DAS Draw-A-Secret. 14

FAR False Acceptance Rate. 17

FRR False Rejection Rate. 17

FS Floor Sensor. 18

GAS Graphical Authentication System. 2

GUI Graphical User Interface. 2

HCI Human Computer interaction. i

kNN K-Nearest Neighbors. 7

MV Machine vision. 18

PC Personal Computer. 2

SVM Support Vector Machine. 7

TNI Transparent non-intrusive identification. 19

VR Virtual Reality. i

VRAS Virtual Reality Authentication Systems. 3

WS Wearable sensors. 18

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The security of information has never been an easy task, and for decades any secure system is just an incident away from being made vulnerable or useless, and human factors have always been the weakest link. The term security is diverse and all-encompassing, covering algorithms and various systems of encryption, including user interfaces. The challenges of providing adequate consumer and product security have grown exponentially as mobile devices rapidly have become the key computing platform. In the span of 30 years, mobile devices have transformed how people access business and personal information; it has become obvious that security systems must be user-friendly to enhance their efficiency.

The main source of interaction with the first generation of mobile devices was the physical keypad, and this went mainstream with the introduction of Motorola mobile devices in 1973 (see Figure 1.1a) using the T9 keyboard layout which was adapted from desktop phones of that era because user interaction at the time involved inputting numeric values to make phone calls or respond to tone-based selections. The importance of securing mobile devices became more evident as the usage of the devices became ubiquitous [82]. The T9 keypad based mobile devices usually required passwords limited to 4 to 6 digits, which greatly constrained password space. However, the later introduction of QWERTY keypads made popular with the release of business communication mobile devices such as the Nokia Communicator 9000 [98] in 1996, the Blackberry 850, and Palm Treo corporate business smartphone (see Figure 1.1b) circa 1999, allowed for a larger password space as a result of the QWERTY keypad‘s alphanumeric qualities, and thus both the need and

(a) (b) (c)

Figure 1.1: **Generations of Mobile devices:** (a) [Left] Motorola MicroTAC phone. [Right] The Nokia 9000 QWERTY keypad phone. (b) BlackBerry 850 QWERTY mobile device. (c) Full touch-screen phone. **(Images [52])**

ability to implement stronger authentication on business devices went into overdrive.

The new password security practices were based on a mixture of alphanumerics and symbols, adapted from the personal computer (PC) world, which was popular and yet cumbersome when used on mobile devices. With these security practices in use, it ensured text-based password would maintain high entropy [78, 135]; thereby making them secure, but less usable and also resulted in issues of low memorability [53], leading many users to avoid using authentication on their mobile devices altogether. In fact, research by Micallef et al. [80], showed that over 64% of users chose not to secure their mobile devices or utilize an authentication system because it was deemed inconvenient and cumbersome [50], highlighting the serious effect of human behaviour, engagement, and interest on security [21]. In addition, copious research has examined the issues of textual password entry on mobile devices and the usability problems experienced due to size and input constraints [139, 78], while other studies have looked into the association of keypad layouts and password security strengths [19, 54].

Second-generation mobile devices used touchscreen-based virtual keypads, which initially required stylus-based interactions, but later evolved into the use of fingers as the resolution technology improved. Full touch-screen mobile devices without an auxiliary hardware keypad appeared with the release of the iPhone in 2007, bringing in an era of interactive GUI (graphical user interface) mobile devices and graphical authentication systems (GAS). As interactive GUI displays became popular and mainstreamed on mobile devices, new sets of graphical authentication systems were developed in an attempt to alleviate the existing usability problems based on psychology studies which revealed humans are more adept at recognizing and recalling images than text [14, 13, 35, 129].

Graphical authentication systems became a viable alternative to the inherent limitations of text-based authentication systems [143, 76, 139, 123], inspired by studies which showed the graphical authentication systems had higher memorability and positive usability values [140, 129, 13, 10]. Although the various approaches, layouts, and designs of these graphical authentication systems were proposed [70, 63, 56, 5], in practice, very few graphical schemes have been widely adopted, and fewer have had the effectiveness of their security properties [134, 9, 27].

Our research involves two very different devices, the handheld, and the VR device, these devices have different form-factors. Handheld devices are very popular and require little or no setup involvement while providing a diverse set of services to the user. These handheld devices do not require the users' full attention or restricted field-of-view (FOV) and are very portable. The VR devices are mainly head-worn and require a lot of setup involvement, full focus, connection to a computer, and attention of the user. Unlike handheld devices, VR devices can only be used in a secure and contained environment due to its immersive and FOV requirements. Furthermore, VR devices are comparatively more bulky and heavier than their hand-held counterparts. Therefore, our approach to designing secure interfaces for these devices is different. For example, because the handheld devices are more susceptible to third-party observation of displayed information, more care is taken to prevent against observation attack, whereas the VR device displays are not easily observed by a third-party, thus another secure interface paradigm is preferred.

Researchers proposed and developed alternative interface layouts and demonstrated different levels of usability and security paradigms through extensive user studies while taking cues from previous studies into the subject matter [27, 146, 25, 5, 34, 134]. In the upcoming sections, we will review previous work and literature on both graphical authentication systems (GAS) and virtual reality authentication systems (VRAS) that shall serve as the bedrock of this thesis. While there are many excellent general reviews [13, 26, 15, 138], with each to some extent reflects the author‘s personal research interest and expertise. Due to the pace of development and breadth of research, a truly comprehensive review is probably impossible, and certainly beyond the scope of this thesis.

1.2 Motivations

The usage of mobile devices in recent years, during the era of graphical authentication systems (GAS) [14], has become a significantly important part of daily processes within our society, with over 23 billion devices owned by individuals globally [141].

While in recent years, giant strides have been made in the field of secure interfaces for mobile devices [22, 78], and these studies have reported different levels of success. Published research in the area of graphical authentication systems currently lacks the consistency and rigorous evaluation of the effects of mobility and encumbrance on security and usability, therefore making it difficult to compare or reproduce results. We are aware of no such work in the literature that examines the finer-grained aspect of usability and the sublime effects of mobility and encumbrance, thus there remains open questions as to acceptable usability levels among mobile device users.

This thesis explores issues involved in developing usable secure interfaces for mobile devices, due to the nature of these devices frequently operating in insecure environments, it provides numerous opportunities for attackers to obtain critical information. We relied heavily on past works by researchers in the field, that have laid foundations in developing solutions that prevent attacks to steal sensitive and private information for malicious purposes. Our motivation is to develop the next generation of interfaces that can provide mechanisms that are both secure and usable, given the size restrictions and usage characteristics for these mobile devices. We expanded the scope to included non-traditionally portable virtual reality devices as they steadily become smaller and untethered.

We examine the research gaps by evaluating the below research questions:

- **Re-conceptualizing mobile device interfaces to make them both secure and usable:** The main challenges of this research question, has been aptly expressed in studies by Davis et al. [30], Liang et al [71] and [94, 25, 63, 118]. They found that graphical authentication systems are susceptible to shoulder surfing, smudge, and capture attacks, while also suggesting that user interface design decisions may intentionally sway user behaviour towards less secure conducts, therefore usability issues often significantly impacts real-world security.

  Our research examined a novel concept, which involves a new graphical authentication system design that would focus on increasing password entropy without sacrificing usability and memorability. We created a novel graphical authentication proto-

type interface named SemanticLock, which uses images as password tokens that allow constructing a semantically memorable story representing the users password. These passwords are entered via the familiar and quick action of dragging and positioning user-defined images on the touchscreen. The interface was designed to incorporate icons that are non-intrinsically related in order to reduce implicit selection biases. In addition, a close proximity sticky feature was added to reduce errors common to mobile devices used on the move. The study involved 63 participants who performed login tasks under various physical postures, motion state and encumbrance. This study included three main methods, firstly we implemented an evaluation of exemplar schemes from the three main categories of graphical passwords on both tablets and smartphones. Secondly, we evaluated the effects of real-world interactions of mobility and encumbrance on all three evaluated graphical authentication systems, collecting performance metrics for further analysis. Thirdly, we adopted the methods of psychometrics and developed a questionnaire, for measuring the comfort of constructing a strong password when using a particular interface. We used expert recommendations to guide the creation and selection of questions and then assessed our questionnaire for reliability and validity; the two essential psychometric properties of a scale. We explored the actual performance factors on the functional graphical authentication systems (SEMANTICLOCK, PATTERN, PIN) while our participants walked in an encumbered and unencumbered state during which they recalled and applied authentication passwords on a mobile device. Novel properties in our SemanticLock design ensured that our graphical authentication system performed better than the other systems compared in this work. This demonstrated that with the proper interface and process design the issue of usability and security can be optimized to be ecologically viable in all scenarios. Our results showed that interacting with mobile devices for authentication purposes is a physically awkward and mentally demanding activity while the user is walking and encumbered, thus gravely affecting overall user security and usability as suggested by other studies [92, 75, 95, 96]. We demonstrated that SemanticLock is superior to the popular PIN and PATTERN authentication systems.

- **The acceptable levels of complexity an interface could have to be secure and yet still usable:**Users express their commands and intentions via interfaces provided by the technology they use. The field of HCI has sought to overcome vari-

ous challenges in interface complexity that cause various security and usability issues. To explore and identify solutions to various interaction challenges while maintaining the same baseline. We developed a novel concept that ports the popular authentication systems into the virtual reality environment, thereby giving us the ability to implement and try numerous heterogeneous interaction methods. The novelty of our second work was to explore the complexity, effectiveness and usability of graphical authentication systems within the virtual reality (VR) environment. We believe that VR and mobile devices, especially smartphones and tablets are intrinsically linked in terms of usage, security and usability factors [151, 102, 109, 62]. The experiment involved 15 participants engaged in creating passwords patterns on the VR PATTERN authentication system using virtual reality hand-held-controller (HHC), LeapMotion, Eyetracking and head-mounted-display (HMD). We evaluated the suitability of porting the popular PATTERN and PIN graphical authentication systems for use within virtual reality (VR) by observing their advantages and vulnerabilities, including the effects of VR interaction techniques/devices. Lastly, we evaluate three levels of threat in regards to shoulder-surfing in an attempt to demonstrate the high resistance to shoulder-surfing. Using the mobile phone versions as control, we did a novel comparative analysis of both environments (mobile phone and VR) and discovered similarities in their metrics. Our results showed that PATTERN and PIN graphical authentication system was well suited for VR. The participants performed equally similar within the mobile device and virtual reality environment, they also performed better using VR interaction methods that were used as an extension of their hands, and the virtual reality implementation of these graphical authentication systems were highly resistant to shoulder-surfing; thereby presented a clear advantage when considering the fact that mobile device graphical authentication systems have very little resistance to shoulder-surfing [73, 111, 55].

- **The technological impediments that make it diffcult to develop secure interfaces:** We explored this challenge with a novel virtual reality (VR) based prototype called BioMove, this concept implements a transparent authentication interface by effectively capturing the biometric movement of the users in a virtual reality environment. High-end virtual-reality (VR) products are striving towards being totally wireless, and this level of mobility widens the useful possibilities in business, entertainment, and private social media activities. Consequently, this freedom of

movement no longer makes it conceivable to expect users to login via a keyboard or other popular tethered authentication methods, but this novel concept, on the other hand, brings the possibility of using motion data from the user's VR environment interactions to determine the identity of the user. Individuals have kinesiologically unique attributes, therefore having behavioural traits that can be used to uniquely identify them in a secure, transparent and non-intrusive manner. We first created a virtual reality environment and conducted a 15 user study where our participants performed a series of controlled tasks (grabbing, rotating, dropping) that could be decomposed into unique kinesiological patterns while capturing and monitoring their hand, head, and eye gaze data. Our result shows the identification confidence values of factor 0.98 and classification accuracy of 99.7% were obtainable using machine learning classification methods such as kNN or SVM. This demonstrates the possibility of using motion in VR as a biometric discriminant thereby adding a layer of transparent authentication that allows these VR applications to be securely used by multiple users without any perceived inconvenience.

Our three major works explore the significant effects of user interactions on the effective security and usability of mobile devices. In our first study we determined various baselines by comparing our novel SemanticLock with two currently popular authentication systems that were used across the other works. The interface design and data obtained from the first study was used to define the parameters for the second study. The second work examined the practical effects of different interaction modes in a virtual reality (VR) environment, using the PATTERN and PIN authentications systems that were ported into VR from the first study, and included the study results been used as a baseline for this second study. The third work, while focusing on usability was conceptually different in approach and process although it utilised the virtual reality environment to explored using the human interactions itself as a resultant security.

1.3 Overview of the Thesis

1.3.1 Contributions

In this thesis, we aim to improve the overall performance of authentication interfaces for mobile devices by ensuring they are both secure and usable. The contributions of the thesis are :

- Design of a graphical authentication system, that employs semantic graphical mnemonics to improve the balance between strong security and better usability while accommodating the interference elements of mobility, hand-input postures, and encumbrance.
- Design and implementation of the popular PIN and PATTERN authentication systems and porting them into the virtual reality environment. This allowed us to evaluate the security, usability, interface and interaction challenges by providing numerous heterogeneous interaction methods within the virtual reality system.
- Design and implementation of a transparent authentication system based on the unique kinesiology features of the user within the virtual reality environment. Biometric authentication provides a highly secure and high usability factor due to its inherent transparent nature.

1.3.2 Organization of this Thesis

The thesis is organized as summarised below:

- **Chapter 2:** This chapter reviews background knowledge and related work of this thesis. We first introduce Alphanumeric (Text-based) Passwords, especially the PIN and QWERTY implementation on mobile devices. Then, we introduce Graphical Passwords, 3D based Passwords, and Biometric Authentication. Finally, we review the state-of-art.
- **Chapter 3:** In this chapter, we introduce SemanticLock, a simple, fast, and memorable single factor graphical authentication approach for mobile devices. The purpose of this novel graphical authentication system was to explore the hypotesis of reconceptualizing mobile device interfaces to make them secure and usable, and to that effect, SemanticLock uses a set of graphical images as password tokens that

allow constructing a semantically memorable story representing the user's password. Passwords are entered via the familiar and quick action of dragging and positioning user-defined images on the touchscreen. It is well known that for (un)locking mechanisms such as PIN or PATTERN, users tend to pick memorable passwords such as dates or simple (often regular) patterns. This practice by users significantly reduces the effective password space for these mechanisms. The authentication strength of SemanticLock is based on the large number of possible semantic constructs derived from the positioning of the image tokens and the type of images selected. Results our study comparing SemanticLock against other authentication systems show that SemanticLock performs similarly to PIN and PATTERN in usability, while have significantly increased memorability and security.

- **Chapter 4:** In this chapter, we explored (1) the suitability of porting the popular PATTERN mobile device authentication system for use within virtual reality (VR) by observing the advantages and vulnerabilities. (2) The effects of the interaction devices such as the hand-held-controller (HHC), the LeapMotion sensor, EyeTracker and the head-mounted-display (HMD). Our study is in three-folds, a web study, mobile device study and a VR study to evaluate the speed,login errors, usability of the PATTERN authentication system in VR and handheld environment for comparison. Lastly, results from the VR shoulder-surfing indicates that the VR implementation of PATTERN has a high resistance, and the Login speed was comparable to that of handheld mobile devices obtained from our research in Chapter 3.

- **Chapter 5:** In this chapter, we present a user study where our participants performed a series of controlled tasks that require physical movements (such as grabbing, rotating, dropping) that could be decomposed into unique kinesiological patterns while we captured and monitored their hand, head, and eye gaze data within the VR environment. The need for secure, transparent and non-intrusive identification mechanisms in VR is important to facilitate users' safe participation and secure experience. We present an analysis of the data and show that this data can be used as a biometric discriminant of high confidence using machine learning classification methods such as kNN or SVM, thereby adding a layer of security in terms of identification or dynamically adapting the VR environment to the users' preferences. We also performed a whitebox penetration testing with 12 attackers, some of whom were physically similar to the participants. We are able to obtain an average identification

confidence value of 0.98 from the actual participants' test data after the initial study and also a trained model classification accuracy of 97.2%. Penetration testing indicates all attackers resulted in confidence values of less than 50%, although physically similar attackers had higher confidence values.

- **Chapter 6:** In this chapter, we examined the purpose of our research and how different components and experiments fit together to attempt to answer the research questions based on our hypotheses. The results and knowledge from these experiments were used as a foundation for further evaluation as we evolved our research through various user environments such as from mobile phone devices into virtual reality devices. We concluded this chapter with a look into the possible limitations and directions for future work of our research.

1.4 List of Publications

1.4.1 Publications Published

1. I. Olade, C. Fleming and H. Liang,"BioMove: Exploration of Biometric identification from human Kinesiological activities in the Virtual Reality environment." https://doi.org/10.3390/s20102944 ***(published May, 22 2020)***

2. I. Olade, H. Liang, C. Fleming and C. Champion "Exploring the Vulnerabilities and Advantages of PATTERN or PATTERN authentication in Virtual Reality (VR).", 2020 ACM 4th International Conference On Virtual and Augmented Reality Simulations (ICVARS 2020), Sydney, NSW, Australia, 2020. https://doi.org/10.1145/3385378.3385385

3. I. Olade, H. Liang and C. Fleming,"A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays," 2018 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced & Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation (SmartWorld IOP2018), Guangzhou, 2018, pp. 1997-2004. doi: 10.1109/SmartWorld.2018.00334

4. Z. Yu, I. Olade, H. Liang and C. Fleming,"Usable Authentication Mechanisms for Mobile Devices: An Exploration of 3D Graphical Passwords," 2016 International

Conference on Platform Technology and Service (PlatCon), Jeju, 2016, pp. 1-3. doi: 10.1109/PlatCon.2016.7456837

1.4.2 Publications in Submission

1. I. Olade, H. Liang and C. Fleming,"SemanticLock: An authentication method for mobile devices using semantically-linked images" ***(Submitted to "IEEE conference on communications and network security".)***
   [Chapter 3 of Thesis]

2. C. Champion, I. Olade, H. Liang, and C. Fleming. "The $Smart^2$ Speaker Blocker: An Open Source Privacy Filter for Connected Home Speakers." Privacy Enhancing Technologies Symposium **(Accepted pending revisions (21% acceptance rate).**
   Contribution of Author: (1) devices integration; (2) algorithm design; (3)algorithm test

1.4.3 Awards

- Genealogical LinkedData Application Development (Apr 2016 – June 2016). The linked data project won the First prize of Shanghai Library Open Data Application Development Contest(top 1.7%), 20,000 RMB (about £2200+).
  HCI contribution of Author: Complete *top-down* **Android** application development with focus on user interface and interaction methods, App Interface and Logic design, Remote data exchanging, Coding and Debugging.
  Website: http://pcrc.library.sh.cn/opendataContestPresentation.html
  Android App Download Link: http://pcrc.library.sh.cn/zt/opendata/2016/

Chapter 2

Review of Related Work

This chapter reviews background knowledge and related work of this thesis. We first introduce Alphanumeric (Text-based) Passwords, especially the PIN and QWERTY implementation on mobile devices. Then, we introduce Graphical Passwords, 3D based Passwords, and Biometric Authentication. Finally, we review the state-of-art.

2.1 Alphanumeric (Text-based) Passwords

Text-based passwords have been the cornerstone of authentication since the electronic age. They are still the de-facto means of authentication on computer systems and other embedded systems that require secure user interactions. Various standard security practices are in use to ensure text-based passwords maintain high entropy which may make them also paradoxically, less secure, less usable and experience memorability issues [53, 78].

2.1.1 Physical mobile device keypad

The first generations of mobile devices had physical keypads as their main source of user input. Since the first handheld mobile phone was demonstrated by Motorola in 1973 (see Figure 1.1a), the problem of securing access to these mobile devices has been evolving. The T9 keyboard originally developed by Tegic Communications was the main-stay of user input, using the numeric PIN as the password. As at that time, most user inputs involved inputting numeric values to make phone calls or respond to tone-based selections. The importance of securing mobile devices especially mobile phones was not realized until

these devices became ubiquitous and increasingly held more user information [82]. With the debut of the first QWERTY mobile smartphone, the Nokia Communicator 9000 [98] in 1996, authentication of mobile devices came to the forefront of many manufacturer designs.

2.1.2 Virtual touch-screen mobile device keypad

Mobile devices such the Apple Newton MessagePad was introduced in 1993 as a productivity tool, it displayed an on-screen virtual keypad and required a stylus for interaction. Similar devices such as the Palm Pilot was released in 1996 but were not quite widely used. Full touch-screen mobile devices without auxiliary keypad support did not appear mainstream until the release of the iPhone in 2007. The virtual keypad used on these fully touch-screen based mobile devices had the same security and user problems as their physical counterparts and in some cases, as explained by [131] induced new forms of security weaknesses.

2.2 Graphical Passwords

With the introduction by G. Blonder [14] of graphical authentication as an alternative to textual knowledge-based authentication systems, graphical password authentication methods validate the user of the mobile device using certain visual representation displayed on the mobile device screen. Furthermore, in graphical passwords, the natural ability of people to process, retain and retrieve visual information [1] has been leveraged on to ensure the selection and use of more secure password profiles [134, 13], similarly according to Biddle et al. [13] studies have shown that the graphical nature of passwords does not entirely eliminate the problems that plague the text-based password systems and the security offered by these graphical schemes are somewhat inferior to text-based passwords [134]. In contrast, recent studies by various researchers have shown methods that significantly improves the security of graphical password to surpass the security level of text-based passwords and also overcome various vulnerabilities that are unique to graphical passwords without compromising usability. Extensive studies have been done in the past in regards to graphical passwords, and various papers categorize and examine about twelve schemes [2] while suggesting usability guidelines for these designs [118]. In this context, three types of graphical password systems have been identified and broadly categorized according to the memory process involved; they are: *Recognition based*, *Recall Based*, *Cued Recall based* [13], and we

shall explore the significance of each of these systems.

2.2.1 Recognition based graphical passwords

Recognition based graphical passwords systems task users with recognizing previously selected images from among decoys to login. Proposed recognition-based systems use various types of images, most notably: faces, random art, everyday objects, and icons [13], numerous versions of this scheme such as Passfaces [108] and Deja vu [33] has been explored by researchers and studies by [35] have shown that this scheme has a low theoretical password space compared to text-based password schemes, field studies conducted found that users selected predictable passwords that could be successfully guessed, despite these issues, studies by Dunphy and Nicholson [35] indicate that graphical password has 30% fewer login errors than text-based password systems.

2.2.2 Recall based graphical passwords

Recall based graphical passwords systems are known to be a memory-intensive task due to the fact that the secret diagram or pattern initially drawn by the user has to be entirely remembered and reproduced; studies by Biddle and Chiasson [13] have shown that the task of recalling the graphical password with this system is similar to text-based password, and consequently having comparable theoretical password space with text passwords and the entropy of patterns or diagrams is rather low [134]. Some popular implementations such as Draw-A-Secret (DAS) [54] and Pass-Go [129, 25] which the mobile device PATTERN lock is based on have been extensively studied.

2.2.3 Cued-recall based graphical passwords

Cued-recall based systems exploit various studies that conclude that the human memory holds information that may be available yet inaccessible for retrieval without the proper trigger or catalyst [4]. This system stands on the idea that pictorial indicators can simplify the task of recall for a user [134, 28]. Some popular implementations such as PassPoint [14, 145, 147], Cue Click Points (CCP) [27] and Cued Gazed ClickPoint (CGP) [61, 20, 101, 97] have been extensively studied.

2.3 3D based Passwords

The three-dimensional environment is where humans naturally exist and operate, and as mobile devices double in computing power bi-annually; not much literature exists in this subject area but researchers have proposed various schemes of introducing 3D virtual environments into the authentication of mobile devices. Alsulaiman and Saddik [4] proposed detailed steps in setting up such 3D virtual environments; meanwhile, very little research has been done towards usability on actual everyday mobile devices. It has been suggested that 3D passwords will eliminate all issues such as shoulder surfing, low entropy, brute force attack and small theoretical password space suffered by graphical passwords and textbased passwords respectively. Other researcher confirmed that the 3D environment allows for the same security lapses that exist in the real world, such as hiding a key or password token under a virtual foot mat; while Yu, I. Olade et al [151] and Odoh et al [100] argued that best real-world practices will take place as the 3D password system proliferate, and a lot of "story and role-playing" with interactive 3D objects will be commonplace, further studies by [151, 103, 87] using virtual reality (VR) and Leap Motion [55] hardware support the claims that the 3D password scheme will increase significantly the theoretical password space. We strongly believe further research and field studies are needed to solidify the practicality of this 3D password system.

2.4 Virtual Reality

In the area of Virtual Reality (VR) authentication, various research has been mainly focused on the *What you are* aspect of the authentication paradigm. Biometric authentication research [109, 119, 114] is very popular for VR because virtual reality inherently exposes various biometric properties of the virtual reality user and these studies are gaining popularity. However, there is growing hesitation in biometric authentication for privacy and data safety reasons. This thesis focuses only on the well known *knowledge-based authentication* in virtual reality systems.

A study by Yada et. al [148] using PIN authentication in augmented reality systems found encouraging results even though the password entry time of this study was five times higher than using PIN on a standard mobile phone. The researcher suggested that visual cues and the reaction time of the Google Glass device were a contributing factor. A recent study by George et al. [45] evaluated the security and usability of PATTERN and PIN

within the VR environment. The study involved 25 participants, they found that usability was comparable in performance to the mobile version of PIN and PATTERN. Although their study was analytically sound, it did not evaluate the shoulder-surfing threat and lacked a direct comparison to an actual mobile device study involving PATTERN and PIN.

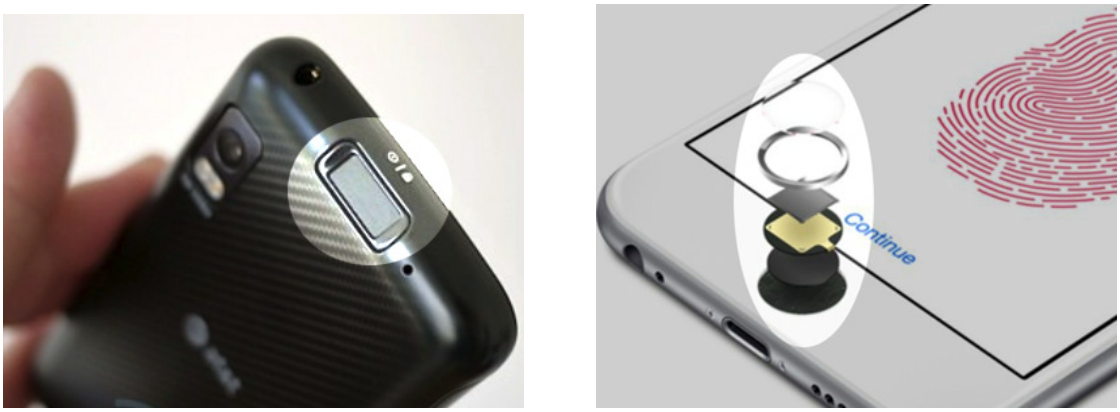
2.5 Biometric Authentication

Biometric authentication uses the distinctiveness of the user's characteristics to determine valid users. These characteristics could be either *Physiological* or *Behavioural*, and in recent years various mobile device manufacturers have implemented some form of biometric authentication in their products. Currently, the most common form of physiological biometric systems employ the use of fingerprints, iris patterns and facial recognition, likewise behavioural biometric systems employ the use of data captured as the user naturally interacts with their mobile device in ways such as keyboard stroke patterns, gait, and movement. Hence it is gaining popularity as the system for implicit, non-intrusive and progressive authentication. While other knowledge-based methods and token-based methods require the users to remember or bring along their secret password tokens, biometric systems have no memory load or carry along requirements. A study [29] found that 98% and 75% of mobile device users consider fingerprint and facial authentication to be highly secure.

2.5.1 Physiological Biometrics

Fingerprint

Fingerprints are outlines on the fingers that are composed of valleys and ridges. The various fingerprint capture technology in use extracts unique minutiae features from the user's finger using a wide variety of imaging technologies. The extracted information is stored for future authentication uses. The emergence of fingerprint technology into mobile devices came with the release of the Fujitsu Mover F505i series [44, 43] in 2003, the Motorola ATRIX [47] (see Figure 2.1a) android phone in 2011, and Apple TouchID [8] in 2013 (see Figure 2.1b), thus brings this technology into the mobile phone mainstream market. These phones required the user to place their password finger on the fingerprint sensor to perform login and other authentication functions, its usage was seamless and unobtrusive.



(a) (b)

Figure 2.1: (a) **Mobile Phone FingerPrint authentication:** Motorola Atrix Fingerprint enabled mobile phone. (b) **TouchID FingerPrint System:** Ergonomically designed finger sensor in IPhones. **(Images [51])**

2.5.2 Behavioural Biometrics

Motion

Motion tracking in mobile devices has been made possible via detection by embedded gyroscope and accelerometers. Gyroscopes are used to measure orientation and angular velocity. This allows mobile devices to track the six degrees of freedom, whereas accelerometers measure accelerative forces and changes in acceleration. Various implementation of biometric authentication exists using these motion detection techniques and while many have promising FAR and FRR, they still require active user participation. Fantana et. al [38] demonstrated a mobile air signature biometric authentication concept, with the motion path detected by the internal accelerometers or gyroscope and conclusively demonstrated a 7% FAR and 10% FRR but the user interacting with the process was publicly visible and not well suited for transparently recurrent biometric authentication. Other research by [64, 40] demonstrated transparent actions such has *phone from pocket*, *phone to head* movements emphasizing the biometric authentication factor of such activities with a high degree of success.

Gait

Gait recognition is the ability to uniquely discriminate the pattern of locomotion of a person. This process is technically mature and has been implemented in many sectors using machine vision [39] (MV), wearable sensors [59] (WS) and floor sensors (FS) [86, 57, 136]. Features like stride width, stride length, swag sway, foot-knee angles, and sound [18] have been collectively used to measure gait and create a discriminating factor for identification purposes in an unobtrusive manner. Mobile devices are essentially wearable sensors since they are worn or carried on the user's person. The placement of these mobile devices determines what type of data can be acquired, and over the years research has been done with the mobile devices placed in the pocket, a belt holster, a shirt chest pocket or held in the hand [112]. In an experiment, Fantana et. al [38] compared the accuracy of the data collected using an Android mobile phone and a professional camera-based high-end motion tracking system [105] and found that the data was similar enough to be used for biometric authentication purposes.

2.6 Biometric Authentication in the Virtual Reality Environment

In the virtual reality environment, the head-mounted display (HMD) is a display device, worn on the head that has a small optic display in front of the eyes (see Figure 2.2). It takes up the entire field of view of the user or at least ensures that whatever the HMD is displaying is always in the field of view of the user. The HMD has many uses in areas such as gaming, aviation, engineering, and medicine. In recent years HMDs have been popular as XR (Virtual, Augmented and Mixed Reality) devices. However, historically HMDs served as auxiliary display devices and had limited mobility because they were tethered to a personal computer (PC) and the security system of the PC served their usage. Recently, the XR headsets are enabling a wide range of new opportunities for the users. These users need to seamlessly authenticate their identity while visiting virtual shopping malls or virtually playing games and making purchases, therefore having facial biometric authentication built into HMDs is naturally a better solution. Fully mobile, untethered HMDs with independent operating systems such as Microsoft HoloLens [85], Oculus-Go [99] and Lenovo's Mirage Solo [66] are *mobile devices* that could be more secured with facial biometric authentication. To the best of our knowledge, we have not found any HMD devices that implement facial

Figure 2.2: **Head Mounted Display (HMD)**. The head-mounted displays used mainly for Virtual, Augmented or Mixed Reality allows Periocular, Ocular Surface Vasculature (acrshortOSV), Iris and Retina methods of biometric authentication due to its form-factor. **(Images courtesy of Getty Images)**

biometrics authentication. Studies by [88, 150, 124, 151] investigate different approaches to authenticate HMD users, but they explored methods that did not use facial biometrics for authentication. Our research indicates that the minimum hardware components required to implement facial biometrics would be a *visible light camera*, an *infrared emitter*, and an *infrared camera*. A few commercially available HMD such as the FOVE [41], HTC Vive-Tobii Pro [132] and HTC Vive [3] *(using a 7invensun upgrade kit, called aGlass)* implement infrared-based eye tracking, which allows users to have more immersible experiences using the HMD because the users can navigate and control the device with the eyes.

Another advantage of the virtual reality environment is the ability to implement other forms of biometric authentication schemes, which may involve the use of hand-held-controllers (HHC) in addition to the HMD to track kinesiological movements that are biometrically discernable. We envision an HMD device such as the newly released mobile Android-based Oculus-Go [99] or Lenovo's Mirage Solo [66] which allow full untethered movement being used for this model of authentication. Traditionally identification has been a distinctively obvious and sometimes intrusive process, and the users are certainly aware of these processes. Transparent non-intrusive identification (TNI) is a process that attempts to extract identifying information from the user's activities or from attributes freely exposed by the user while doing these activities, and therefore the system is able to continuously authenticate the user. Most TNI systems in the current literature use behavioural patterns

such as gait [72, 128], typing [83, 79, 115], eye movement [81, 36], touch [121, 42] and brainwave EEG patterns [89, 120]. More recently, research and commercial systems have harnessed users' physical facial features and their finger biometric attributes to develop TNI systems. Although physical biometric attributes from users' face and fingers are more accurate relative to behavioural biometrics, they are generally more intrusive to the users. As an example, for a single-point fingerprint sensor to continuously authenticate the user, the finger must pass frequently on the sensor, a requirement which might be considered intrusive or disruptive for certain tasks or users. Alternatively, user based behavioural attributes such as touch patterns, gait, eye movement have no restrictive requirements and biometric data needed for identification can be captured transparently as the user types, walks or touch the system during an activity.

In Sluganovic *et al.* [125], the authors developed an identification system that uses visual stimulus to elicit reflexive eye movements based on fixation, saccade, and acceleration cues, in a predictable manner that supports the extraction of reliable biometric features. Using a gaze tracking device with a randomly generated stimulus, to prevent replay attacks, the researchers achieved an equal error rate of 6.3%. Head movement and head pointing studies have been performed by [69, 116, 68] as a means to support biometric identification. Recently, an interesting research by Mustafa [87] *et al.* used only the sensors of an HMD to track users' behaviour patterns while they followed randomly appearing balls in a VR environment while navigating only by head movements. They achieved an equal error rate of 7%. Furthermore, other studies by Li *et al.* [69] recorded a high degree of accuracy in identifying participants while they nodded when listening to music. Similarly, in a study by Yi *et al.* [149], a set of six head-explicit gestures that included making a circle, triangle, square and three kinds of lines were used to authenticate participants who used their nose as a pointer to perform gestures. The study obtained identification accuracy as high as 92%.

We believe future research will be focused on implementing a seamless unobtrusive biometric authentication mechanism for VR.

2.7 Conclusion

In this chatpter we reviewed background knowledge and related work of this thesis. We first introduce background concepts such as alphanumeric passwords, especially the PIN and QWERTY implementation on mobile devices. Then, we introduce graphical passwords, 3D

based passwords, and biometric authentication. Finally, we review the state-of-art in biometric authentication within the virtual reality environment because it allows us to explore various user interaction methods. Biometric authentication has gained popularity as the system for implicit, non-intrusive and progressive authentication because it has no memory load or carry-along requirements. The miniaturization of advanced facial authentication hardware systems into mobile devices such as mobile phones and head-mounted displays (HMDs) used for VR/AR/MR has made biometric authentication seamless. This thesis examine the possible application of these technologies within virtual reality and the most recently released mobile phone devices on the market, while considering the challenges, findings and advances within our scope of research.

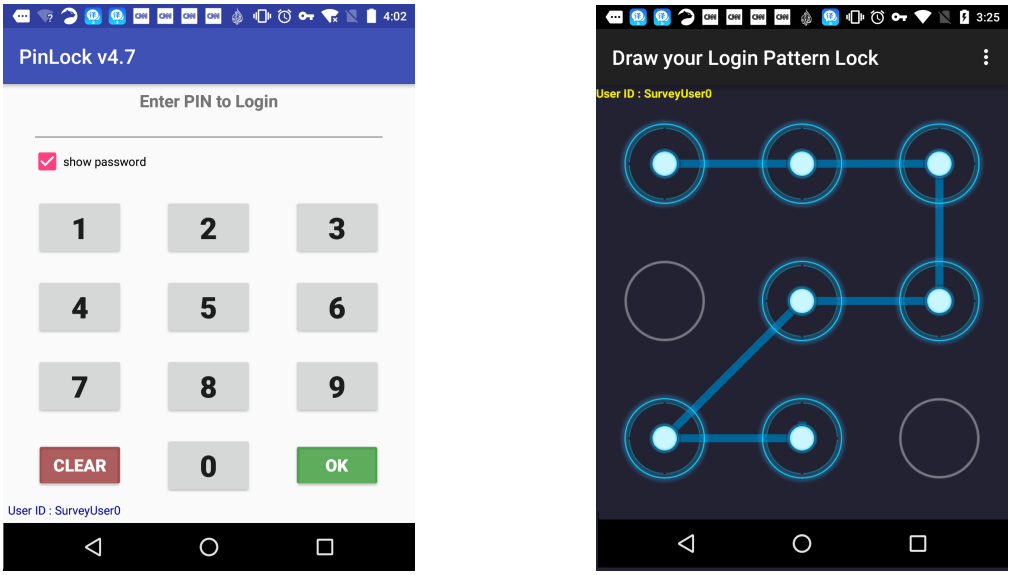
Chapter 3

SemanticLock: A Story-based Graphical Authentication System

3.1 Introduction

Mobile devices, being the de facto personal communication device, are ubiquitous within our society [141]. We depend on these devices to store substantial amounts of confidential information and perform activities such as emailing, social networking, personal internet banking, and entertainment. All mobile devices manufactured in the last decade come with a default set of authentication or login mechanisms. Research by Micallef et al. [80], shows that over 64% of users chose not to secure or use an authentication system on their mobile devices [50].

In general, research has shown that the behaviour, engagement, and interest of the users have a major impact on the effective security level of their mobile devices, with many users preferring to sacrifice security for convenience [21]. The uniformity of the distribution of user passwords within an authentication system's total password space is a practical measure of the usable level of security of that authentication system. Guessing or dictionary attacks on user passwords are less successful when authentication systems have a uniform distribution of user passwords. Studies by [22, 78] indicate that the distribution of text passwords chosen by users effectively have a very low entropy, meaning that the actual space of passwords most users choose from is much smaller than the total space available. The above observation is known to affect prominent authentication systems such as PIN [49, 60, 138] and PATTERN [152, 134, 49, 140] and has been extensively studied, with a



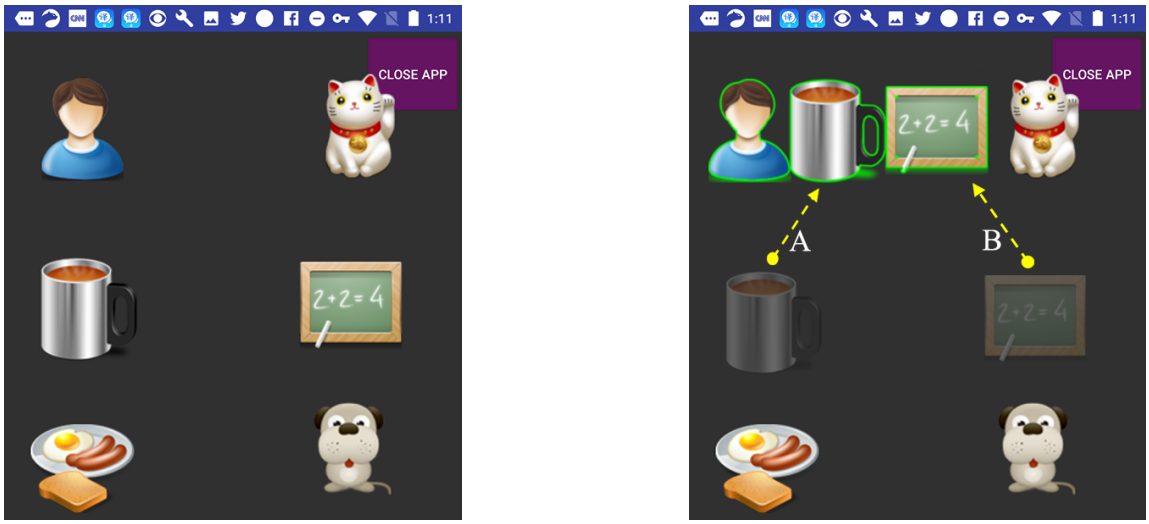
(a) PIN (b) Pattern

Figure 3.1: **Prominent mobile device authentication systems**: The PIN and Pattern authentication systems are popular with mobile devices that have GUI touchscreen-based systems.

large body of existing literature.

The PIN authentication system (see Figure 3.1(a)), which is a numeric display of numbers inputted by discrete touches on the screen and the PATTERN authentication system (see Figure 3.1(b)), which is a "grid-like" display of nodes whose password pattern is selected by a continuous finger movement across the screen to connect the secret password nodes, are both plagued with numerous usage and security issues [1, 84, 7, 152]. Fortunately, the popularity of touch-screen based mobile devices allows for graphical authentication techniques that offer possibilities of providing passwords that are effectively stronger than text passwords. Recently, researchers have developed and studied various graphical authentication systems [5, 141, 30, 10, 127] that take advantage of the inherent human memorability properties and have attempted to mitigate factors such as low password distribution, low unlocking speed, medium-to-low entropy, and other biases, without much success.

In this thesis, we present SemanticLock, a single factor graphical authentication method for touchscreen mobile devices. Our solution works by providing the user with a way to



(a) (b)

Figure 3.2: **SemanticLock**: (a) Default view for login and setup. (b) Login: the user drags two images to meet the third image. In this case, Cup is dragged to the right side of Person ***(movement "A")***, then Blackboard is dragged to right the side of Cup ***(movement "B")***. Login can be done with *two quick* movements (**A,B**).

unlock their mobile devices by joining images via discrete and continuous finger movements to create a semantically memorable story that represents a password (see Figure 3.2(a)). SemanticLock can create a strong memorable password with just two discrete finger movements allowing the user to construct a semantically meaningful password quickly (see Figure 3.2(b)) from the provided images. In the SemanticLock scheme, a password is a sequence of k images selected by the user to make a "story" from a single set of $n > k$ images. These non-intrinsically related images are placed in position p in one of four locations around a pre-existing image. For mobile devices such as smartphones, six images *(n=6)*, allows for comfortable usage, yielding 14,400 possible passwords, which is similar to a 4 digit PIN. Furthermore as previously mentioned, users drag and join at least three of the provided images to construct their password (see Figure 3.2(b)), the semantic story could be *"I drink coffee and study"*. The location of each image in the group constitutes part of the password algorithm. Other password patterns are displayed in Figure 3.3(a) and Figure 3.3(b), these pictures are just examples and they can be customized by the users. Additionally, Figure 3.3(c) shows how easy it is to create a new password.

(a) (b) (c)

Figure 3.3: **SemanticLock:** (a) (person-breakfast-coffee: *"I eat breakfast with coffee"*). (b) (cat-breakfast-dog: *"cat shares meal with dog"*) (c) (person-breakfast-dog: *"I eat breakfast with my dog"*)

Our technique strives to improve on memorability [25, 49] while significantly increasing unlock speed, password distribution, and password entropy. To increase the entropy of the selected password distribution, we ensured that we reduced password image bias by performing three weeks of preliminary online study with the goal of eliminating disproportionately popular images and image pairs. In that study, our participants were required to match intrinsically related password images from a set of 40 images that were initially selected from diverse categories (see Figure 3.4). We subsequently obtained 6 *"least intrinsically"* related images from that study and used them during another 2 weeks password creation study (see Figure 3.5(a,b)).

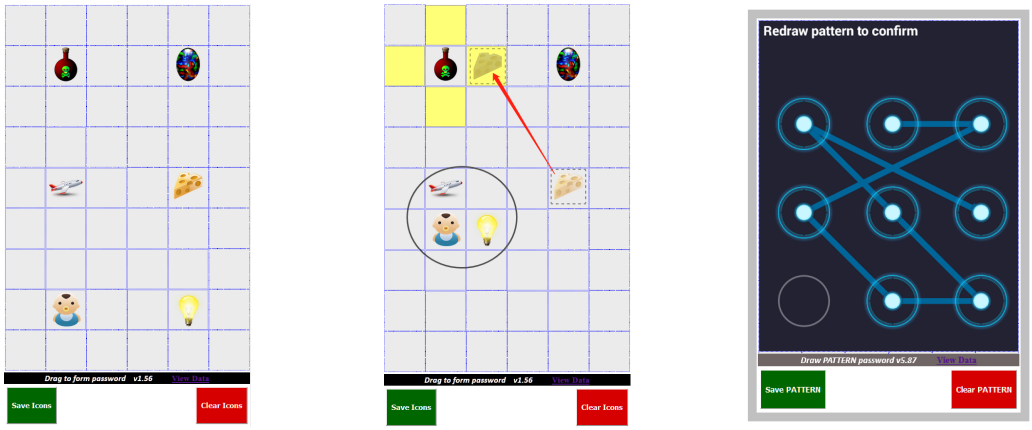
3.1.1 Challenges and proposed design approach

In designing the SemanticLock system, we set out to develop a system that was easy to use, very secure and quick to login. Therefore our primary focuses were speed, ease of use, memorability and high entropy. In addition, we wanted our solution to perform consistently across all usage environments and situations our users may find themselves, and to that end, our study involved scenarios such as sitting, walking unencumbered and encumbered. We ensured that SemanticLock would require only two distinct swipes or finger movements to construct a login password. We implemented a *close proximity* "sticky" feature that visually highlights the two images that are in close proximity to each other while the user is actively dragging one of the images. If the user releases this image it

Figure 3.4: **Related Icon Pairing Web Interface:** Our online web page allowed our participants to select 2 icons that they felt were related. They dragged these icons into the "pairboxes".

automatically "glides" towards the closest image and "sticks" to it. This feature greatly reduces errors caused by unsteady finger movements and increases overall login speeds. SemanticLock also inherits both the discrete and continuous finger movement properties of the PIN and PATTERN authentication system respectively. However, in contrast to PATTERN, SemanticLock only requires two short swipes rather than one continuous long swipe thereby minimizing the time needed to complete a login session or recover from errors [113]. SemanticLock is inherently resistant to smudge attacks because the location of its passwords tokens on the screen is irrelevant to the creation of the password, whereas the PIN and PATTERN authentication systems are susceptible to smudge attacks [49, 152]. Furthermore, to assess our system and get a comparative evaluation, we selected the two most widely used graphical authentication systems as control and conducted a user study over a three weeks period to compare our SemanticLock authentication system against PATTERN, PIN, and PIN-Shuffled authentication systems (see Figure3.1). As such we have formulated the following hypotheses:

Hypothesis H1: We expect that the results obtained from the SemanticLock system will be comparatively similar or relatively close to those of the PATTERN authentication system, despite the fact that most of our users have prior inherent knowledge and



(a) (b) (c)

Figure 3.5: **SemanticLock Web-based Password Creator**: (a) Default view of icon placement. (b) **Creating Password:** the user drags the "cheese" to meet the stationary "bottle" icon. In this case, "cheese" is also dragged to the right side of "bottle". Lastly, a three-icon password is shown ***(see black circle).*** (c) **PATTERN password Web Interface :** Participants were requested to create various pattern passwords.

familiarity with the PATTERN authentication system.

Hypothesis H2: We also expect the PIN system to firmly supersede the SemanticLock system and be closer in performance to the PATTERN authentication system.

Hypothesis H3: We predict that the SemanticLock will supersede the PIN-SHUFFLE in regards to unlock speed. Both authentication systems are inherently resistant to smudge attacks.

Within the study, we utilized the dataset we collected during the initial three-week period, and we showed that while SemanticLock can be practically more secure than the PIN and PATTERN authentication systems *(see section 3.4.1)*. Its usability performance was also better than the PIN and similar to PATTERN under normal circumstances *(see section 3.4.5)*.

The rest of this chapter is structured as follows. In section 3.2, we describe our methodology in more detail, such as the preliminary web-based studies, the graphical password schemes that we evaluated during the mobile device study, and our experimental design. In section 3.3, we present our data sources and data collection models. In section 3.4 and

3.5, we discuss issues and findings and present our results. In section 3.4.1, we explored the password strength and practical entropy levels of the PATTERN and SemanticLock authentication systems. In section 3.6 we mention limitations and conclusion of the study.

3.2 Methodology

We employed two strategies in an attempt to achieve the desired features and functions of our previously described SemanticLock system. Pre-system development analysis and experiments are required in order to derive initial icon sets. Therefore two studies were conducted, a web-based study and a mobile device study. Both studies are discussed below.

3.2.1 Web-based Study

A major aspect of our research is determining the types of icons that will be used in our SemanticLock authentication system, these icons were expected to increase the practical password entropy evaluations of the system (see section 3.4.1). A web-based approach was the most practical method of collecting large amounts of data from a large group of participants. We used the University email system and social media platforms to generate awareness for the experiment, which resulted in a large response. Additionally, a similar web interface was created to collect samples of PATTERN passwords from the same group of participants (see Figure 3.4 and 3.5).

Software and Web Technology

For this aspect of the study, we utilized multiple web-based interfaces that were designed using HTML5, PHP and MySQL database back-end technologies. This allowed us to implement icon drag-n-drop actions and graphical line drawing functions that are common on touch-screen based devices (see Figure 3.6). While web-based experiments are harder to control than in a laboratory or supervised field experiments [13], this channel of data collection met our requirements and offers numerous advantages.

Goals

As part of our goals in the design of our SemanticLock system, our initial intention is to avoid any implicitly induced biases in the researcher's selection of the password icons that may lower the entropy or reduce the achievable password space [31]. In general, security

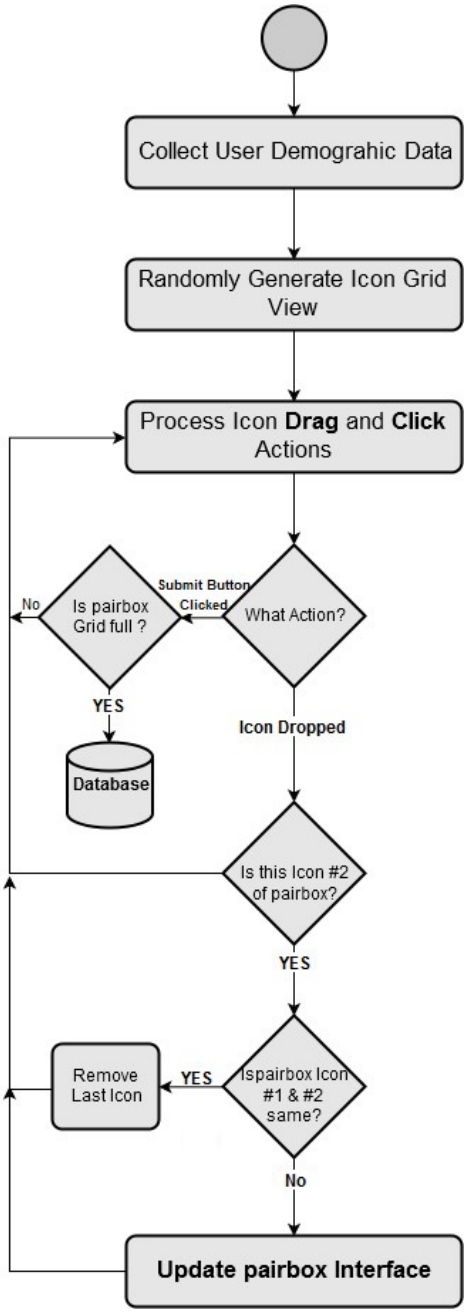


Figure 3.6: **Web Icon pairing flowchart:** Software Process flow of web-based Icon Pairing

experts have observed that an authentication system's *theoretical password space* is never optimally achieved during practical usage [23, 48, 15, 78], and there is also a need to determine the actual *practical password space* that supports the ecological validity of such an authentication system. We defined two stages of the experiment to achieve the above-stated objectives and implemented these stages with two different groups of participants. The output of the analysis of the dataset collected in the first stage was utilized during the second stage. Our purpose for collecting a series of PATTERN password data during stage 2 was to evaluate the distribution and the popularity of certain PATTERN passwords, and also eliminate these common passwords from our PATTERN password selection during the Mobile Device study (see Section 3.2.2).

Participants

For Stage 1: As explained in section 3.2.1, we engaged 372 participants, many were recruited via campus-wide email and social media groups, most were university students, but with diverse age ranges. We also collected other demographic information such as academic background, computer skills and their experience with mobile devices or authentication systems, but this data was not used in the research analysis.

For Stage 2: We engaged 184 participants, many were recruited via campus-wide email and social media groups, 70% were students within the same university campus and the rest were non-students. Our web portal included a 3 minute training video, and each participant was encouraged to watch the video before attempting to create passwords. We advised our participants to create at least 10 passwords each. We also collected other demographic information such as academic background, computer skills and experience with mobile devices or authentication systems, but this data was not used in the research analysis.

Acquisition of independent password icons and common PATTERN Passwords

During Stage 1, our initial process was to provide a set of 40 icons that were drawn from various categories and genres. We explicitly avoided icons that had major gender-oriented colours, and icons with cultural, national or religious relevance. Our participants were then presented with a web-based interface that displayed these icons on a 10 x 4 grid (see Figure 3.4), with each icon randomly positioned in different grid-cells during every selection

session to prevent locational bias. Participants were required to create 10 sets of *"icons-pairs"* that they believed were related by dragging these icons into the provided *pairboxes*, the reason or logic of this relationship was based on their discretion. Each participant was allowed multiple iterations. We analyzed the 3708 collected *pair-datasets* to extract 6 icons that were the least intrinsically related. These *"non-intrinsically"* related icons were used in the next stage of the experiment.

Data collection for the evaluation of practical password space

During Stage 2, our primary goal was to quantify the effect of a participant's choice on the security of passwords chosen. Every authentication scheme has entropy and the strength of such entropy is determined by the probability distribution associated with the password space *(see section 3.4.1 & 3.4.4)*. Ideally, this distribution is approximately uniform. At this stage of our experiment, we presented a SemanticLock web-based interface displaying the six derived *non-intrinsically related* password icons on a 9 x 6 celled grid to our participants (see Figure 3.5(a)). Our participants were required to create several semantic passwords with the password icons by dragging a chosen icon to the *left, top, right or bottom* position of an associated stationary icon (see Figure 3.5(b)). Secondly, the participants were also shown a 3x3 PATTERN web interface (see Figure 3.5 (c)) and were requested to draw 10 different patterns. The web-interface ensured that the user could not repeat patterns within the same session or create patterns with less than 3 nodes. We excluded the PATTERN passwords collected from this stage in our experiment if they exist in the set of carefully pre-decided pattern passwords that met our node count and complexity criteria. At the conclusion of this stage we had successfully collected data about common positional layout of SemanticLock passwords, and also identified a set of common PATTERN passwords that would be excluded from our final Mobile Device study.

3.2.2 Mobile Device Study

Our mobile device study made use of the Android platform. We developed a mobile version (see Figure 3.1(a) and Figure 3.2(a)) of the interface that was used during our web-based study (see Figure 3.5). We also developed Android versions of the Pattern and PIN lock authentication systems since these authentication systems would be our baseline or control conditions for this study due to their popularity and the large body of research literature about their performances. We developed an additional application to help us convey the

testing and survey to our participants in a uniform and consistent way. The process flow of this application is shown in Figure 3.7. It allowed participants to view an initial training video, assigned a unique participant ID that allowed us to correlate data across Login techniques and also presented the pre-survey and post-survey questionnaires in the proper sequences while implementing the Latin square approach to counterbalance the order of the techniques (see Figure 3.8).

Goals

Our objective during this three-week study, which involved participants in an indoor environment, was to collect both qualitative and quantitative data which would provide insight into our participant's perception of the likeability, usability, memorability and login speed of the 3 authentication approaches:

- SemanticLock
- Pattern Lock
- PIN

The prototypes, shown in (Figure 3.1 and Figure 3.2), met our goal of ensuring compatibility with Android 6.0 and above while meeting the requirements of working on phone and tablet form-factors. The training mode option allowed users to receive adequate training and practice before the actual testing. During the testing, a participant's activities such as touches, password tokens, strokes, pauses, timings, aborts, and errors were logged for further analysis.

Participants

We recruited 63 participants from a local university. The data from our pre-testing survey reveals that 51% of the participants were between the ages of 17 to 27 and all our participants were right-handed. All were active users of iPhone (31%) or Android (66%) mobile phones. 55% of them used a phone with a fingerprint sensor, while 17% used the PIN password, 14% used Pattern password and, the remaining did not use authentication. 50% of our participants claim the input hand posture they preferred to use depends on the situation and the app in question; 27% claimed they preferred to use two hands to operate their mobile devices. All participated voluntarily without any financial remuneration.

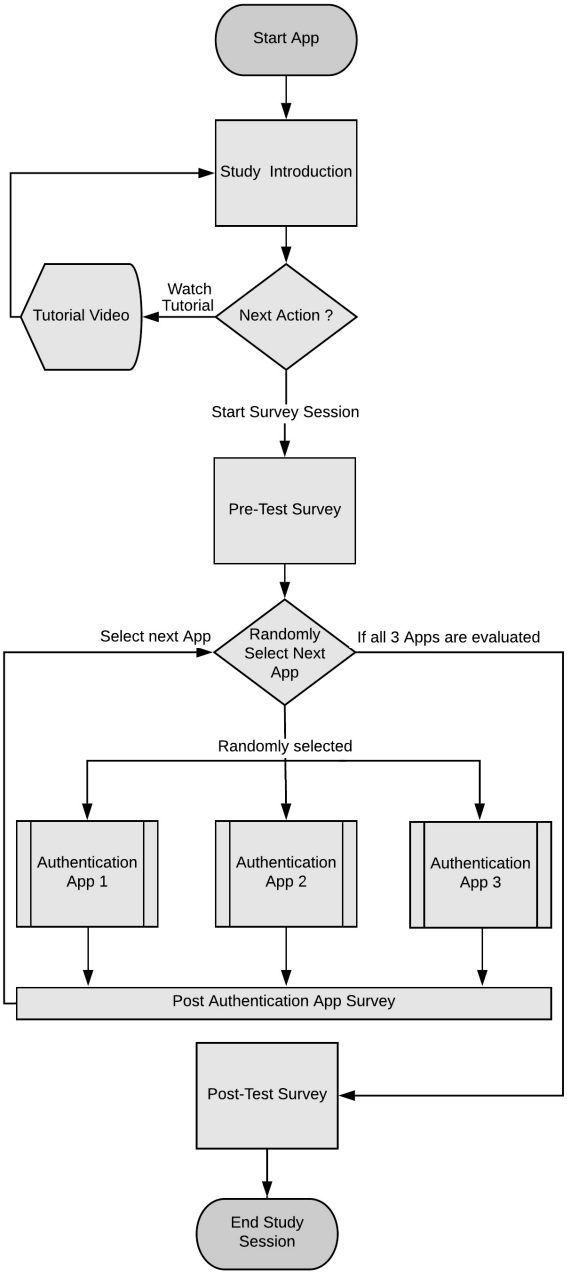
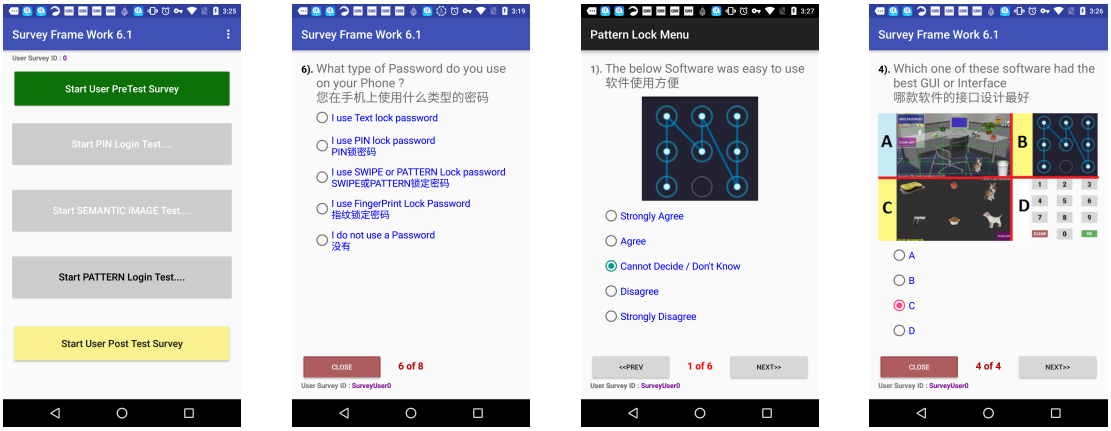


Figure 3.7: **Mobile Device Study:** Flowchart showing the software flow process for the Mobile Device study.



(a) User Study Admin App (b) User Survey Question (c) Post Test In-App Survey (d) Post Test Survey

Figure 3.8: **Survey App Framework**: (a) The survey framework app allowed us to provide a consistent process to all participants. (b) pre-test survey collected user demographics and preferences. (c) Post-test survey specific to the system just tested. (d) The Post-test general survey, to collect user's overall opinions

Experimental Design

Our goal was to compare the three main techniques and their interactions with other independent variables. To do this, we followed a within-participants design. Below are the variables we are tracking:

The independent variables are :

- Technique
- Device Form-Factor
- Physical Posture
- Hand Posture

The dependent variables are :

- Login Speed
- Pre-Login Delay Time
- Error Rate
- User usability and acceptance

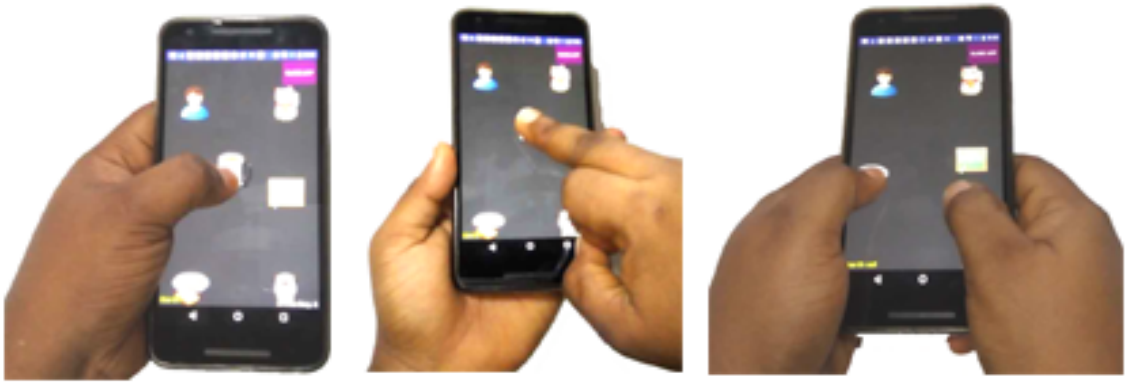
(a) Seated (b) Walking (c) Walking Encumbered

Figure 3.9: **Participants in the Study:** (a) Participant performing a Seated Test using the Tablet. (b) The user is walking unencumbered. (c) Encumbered posture while using the single-hand main thumb input posture.

Technique: Our experiment compared three techniques which are the PIN, PATTERN, and SemanticLock authentication systems. The task required of each participant was to enter the password tokens as fast as possible during each session, while we implicitly collected and tracked data and meta-data for future analysis. We assigned password tokens for each technique so that each participant would use a sufficiently strong password that is properly distributed within the space of possible passwords. We attempted to ensure that the password tokens given for each technique had relatively the same password strength.

Device Form-Factor: Mobile devices are available in various dimensions. We performed our study with a 5.2" LG Nexus 5X phone and a 10.2" Google Pixel C tablet. The tablet was only used during the Seated session (Figure 3.9 (a)) of the experiment, while the LG phone was used for all sessions (Figure 3.9 (b),(c)).

Physical Posture: Studies show that the physical posture of users has an effect on the way they use their mobile devices [90, 95, 91]. Recent studies have shown that walking encumbered or unencumbered and operating a mobile device had significant effects on the



(a) One-handed thumb (b) two-handed index finger (c) two-handed both thumbs

Figure 3.10: **Input Hand Postures:** The most common hand postures when using mobile devices. These postured were tested during the Study. Input postures involving two hands are common due to mobile devices that have larger screens.

usage pattern of mobile devices [126, 93, 107]. Therefore in this study, we included 3 physical postures:

Seated: This posture required participants to sit on a comfortable chair and operate the mobile device on a table and could use one or two hands (see Figure 3.9(a)).

Walking Unencumbered: This posture implied that the person operating the mobile device was also walking but without carrying any other objects with their hands or arms (see Figure 3.9(b)).

Walking Encumbered: This posture took place when participants would operate a mobile device while carrying other items such as books or bags with their hands or arms (see Figure 3.9(c)).

Hand Posture: Hand posture defines how a mobile phone is held when in use by the user. There are 3 prominent input postures: *one-handed preferred thumb, two-handed index finger* and *two-handed both thumbs* (see Figure 3.10). With the advent of larger mobile phone screens, many users have had to change from the one hand input posture to the two-handed input posture [93, 107]

Task and Procedures

Our first step was to inform the participants about the confidentiality of their supplied information and to explain the purpose of the project and the tasks they would need to do. We provided a three-minute training video to each participant (see Figure 3.8a), after which they were allowed to practice each technique a couple of times. They practiced the creation of a password and use the password to login to the mobile device. We emphasized the need for a speedy and accurate login during the actual testing phase.

Week 1 (First Phase): Each participant was required to answer a pre-test questionnaire before commencing the test (see Figure 3.8b). We allowed each participant to choose password tokens for each technique from our supplied list. If the participant entered the wrong password, the application alerted them to enter the correct password again. The average time for participants to complete all techniques (including questionnaires) was 4 minutes. The experiment finished with a Likert questionnaire (see Figure 3.8c) that collected qualitative data about the participants' perceived usability, error-handling, security and likeability of each technique. This week's session was a seated session and the participants used the techniques on the LG mobile phone and the Google tablet. The main independent variables were *technique* (PIN, Pattern, and SemanticLock) and *mobile form factor* (phone and tablet). Each participant had to enter a total of 9 passwords per session, 3 for each technique and participants were allowed a 60-second rest in between techniques to minimize fatigue if there was any.

Week 2 (Second Phase): In the second phase, which occurred a week after, we explored the memorability aspects of the three techniques. We asked the same participants to recall the passwords they had used for each technique the previous week. During this session, we tracked error-rates, type of error, action-delay times and login speed required for our future analysis.

Week 3 (Third Phase): We recalled the participants for a third session that required them to perform login activities while walking around a predefined path within an indoor environment. We followed a procedure similar to the one used by [95, 93] in which they examined the effect of mobility and encumbrance on participants using both one and two-handed interactions on touchscreen mobile devices. The walking speed was paced by a researcher (see Figure 3.11) who used a metronome to ensure a proper walking speed was maintained. After the walking test (see Figure 3.9(b)), each participant undertook the

Figure 3.11: **Pacing the user:** A Pacesetter (Dr. I.A Olade) ***(right)*** keeping the participant ***(left)*** at a steady walking pace with the help of metronome software during a login test.

encumbrance test, which required each participant to walk along a path at a paced speed carrying two nylon bags containing a 100cl plastic bottle while unlocking the device using each technique (see Figure 3.9(c)). The decision to use nylon bags was informed by the research done by Ng et al. [95]. In this phase, we sought to investigate the effect of mobility and encumbrance on the login speed, memorability and input errors while assessing the techniques with the 3 commonly used input postures presented in [107].

3.3 Data Collection and Measurement

We collected data for a number of dependent variables and used this data to evaluate the techniques.

3.3.1 Pre-Login Delay time: Memorability and Usability

Pre-login delay is the elapsed time between when the participant indicated that they were ready to start unlocking the device and the actual time they entered the password. This data provides a view into evaluating the memorability and usability of the system. Studies

by Stobert et al. [127, 144] defined a direct relationship between memorability and pre-login delay time. We analyze this data to quantify the level of memorability and usability.

3.3.2 Login Speed

The time period used to complete each trial of the login process for a technique was recorded. This measurement recorded both successful and failed trials. Login speed was tracked from the moment a participant starts password token entry until the entry was completed successfully.

3.3.3 Error Rate

The error rate was measured as a percentage of failed login attempts to the total number of attempts required to complete the technique's session. The number of failed login attempts during a trial did not affect the number of trials that constituted a complete session.

3.3.4 Subjective Data

We collected *pre-test*, *in-test*, and *post-test* surveys via an electronic questionnaire (see Figure 3.8 (b,c,d)). The questions focused on ease of use, perception of speed, the likelihood of adoption, error recovery, and interface usability. We implemented the questionnaire in electronic form and used 5-point Likert questions for some aspects of the questionnaire.

3.4 Results

The results from this study are in two folds, the data collected from the web-based interface was used to determine security factors for both the SemanticLock and PATTERN, whereas the data collected from the mobile device interface, which are quantitative and qualitative in nature was used to determine usability factors. Our analytical processes are discussed below.

3.4.1 Authentication Password Space, Security and Entropy Analysis

With many authentication systems, users tend to choose passwords that are easy to remember, meaning that they do not select their password uniformly from the whole space

of possible passwords, but instead show a higher probability to choose from certain subsets. For example, PIN users often choose dates that have some significance to them as passwords. The degree of randomness of passwords practically chosen by users is an important factor in determining the security of an authentication system. The level of password randomness is an important factor in determining the uniqueness of a security token. The term entropy has been widely examined in the various existing literature and there exists a large body of work [23, 32] evaluating the entropy of alphanumeric text-based passwords and PIN passwords. Entropy was introduced by C. Shannon [122] *(see equation 3.1)* as a measure of uncertainty of choices. Given a discrete random variable (χ) where N is the total number of observed events and ρ_i is the probability of the i event, while $\sum$ denotes the sum over the variable's possible values, and its denoted by $H_1(\chi)$, which is

$$H_1(\chi) = \sum_{i=1}^{N} -\rho_i \log_2 \rho_i \tag{3.1}$$

The quality of alphanumeric password policies can be measured in terms of entropy (using combinatorial considerations), an analogous measure for graphical authentication systems is certainly desirable. However, various studies, such as those by Uellenbeck et al [134], Tupsamudre et al [133] has explored Pattern authentication security and observed that its practical password space is significantly less than its theoretical password space (see Table 3.1).

Table 3.1: Theoretical Password Space values for Authentication System

Authentication System	**Theoretical Space**
SemanticLock *(3x2)***	14,440
PIN *(6-digits)*	1,000,000
Pattern *(3x3)*	389,112
PIN *(4-digits)*	10,000

**for theoretical password space value of the SemanticLock

The primary attack we are considering is the brute force guessing attack. The objective of a guessing attack is to achieve a high number of match success within a fixed number of attempts, leveraging the knowledge of user password preferences. Studies by [134, 7]

proposed an algorithm called partial guessing entropy [15] (α-*guesswork*), which depicts the success rates as a function of the password distribution space. We use this algorithm to evaluate the security of SemanticLock with respect to guessing attacks.

In order to use α-guesswork, we need to have an estimate of the distribution of user-selected passwords. While the PIN password distribution can be estimated based on leaked password databases or surveys, it is more difficult to obtain this type of data for graphical password systems such as PATTERN and SemanticLock. Instead, we use a Markov model from [134], which is based on the idea that the subsequent token in a password, such as the next node in a PATTERN system, is dependent on the previous token. Therefore, with a given sequence of password tokens, we must determine from the initial probabilities $P(c_1, ..., c_m)$ and the subsequent transitional probabilities $P(c_i|c_1, ..., c_{n-1})$. This data was collected as part of our online survey.

3.4.2 Introduction and Implementation of Markov Modeling

Authentication strength is built on the difficulty level of predicting the future tokens in a password series of a randomly changing system. The Markov chain attempts to model a system state as it changes through time. As mentioned earlier, in order to use the Markov model we must determine the initial probabilities $P(c_1, ..., c_m)$ and the subsequent transitional probabilities $P(c_i|c_1, ..., c_{n-1})$. In this study, we performed a series of analyses based on Markov chains to quantify the security of the Pattern and SemanticLock authentication system using the data we collected during the online survey. We followed closely the data preparation process described in [134], with our dataset split into K=7 disjointed subsets of $S_1, ..., S_7$ and using $S_1 - S_6$ as the *training set* and S_7 as the *test set*. For PATTERN we used n-gram value of n=3 as described in [134], while for SemanticLock we determined that the most common passwords consist of 3 icon sets or subsets (see Figure 3.12) , therefore we also used *n=3* during the Markov analysis. Then, we enumerated all valid patterns, using a recursive algorithm. Finally, we match the output guesses against the test set, recording how many guesses existed in the test set that was provided. Our above methods were used to obtain the results discussed in section 3.4.4 .

$$P(c_1, ..., c_m) = P(c_1, ..., c_{n-1}) \cdot \prod_{i=n}^{m} P(c_i|c_{i-n+1}, ..., c_{n-1}) \tag{3.2}$$

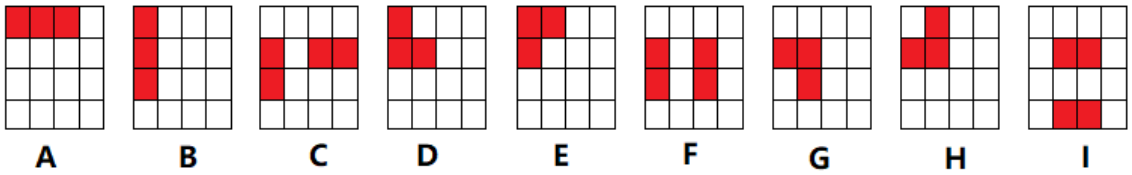


Figure 3.12: **Most common SemanticLock Icon-Pair patterns :** A list of the most common SemanticLock "Icon-Pair" patterns in our user dataset. This was used to select the n-gram value for our Markov model analysis.

3.4.3 SemanticLock Web-based Data Analysis

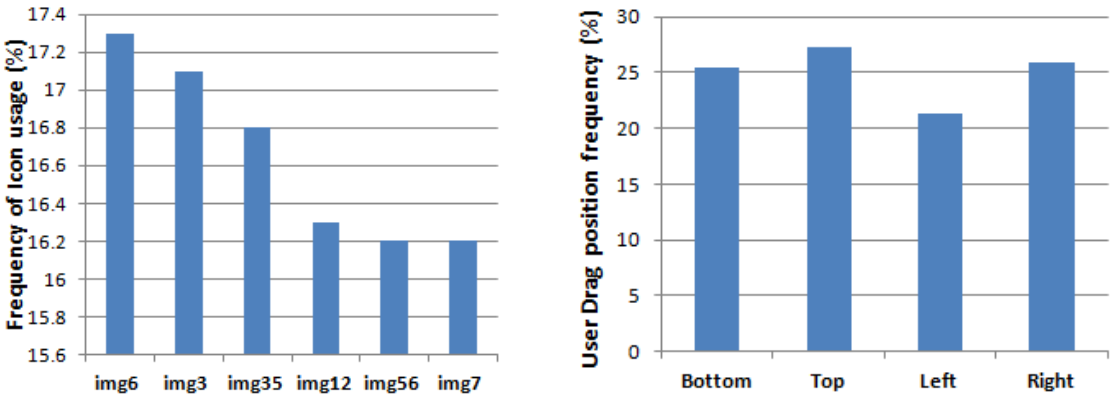
The data collected from the participants during stage 2 of the web-based study was analyzed to confirm that our icon selection method was valid and to derive statistics needed for our Markov model.

Password Icon distribution:

Frequency analysis was performed on the SemanticLock password data sets collected. Each SemanticLock password is made up of unique icons selected from the 6 initial password icons. From our dataset of 1825 semantically created passwords, our analysis suggests that the choice of each of the six password icons is uniformly distributed. (see Figure 3.13(a))

Password Icon-pair position distribution:

Password icons are used to create semantic passwords by dragging a selected password icon to a *"resting position"* next to the stationary password icon. This *"resting position"* could either be the *left, top, right* or *bottom* of a stationary password icon (see Figure 3.5(a) and (b)). We analyzed the collected positional data sets to determine if our participants displayed a bias in their choice of *"resting positions"*. Our analysis indicated that the participant selection of *"resting positions"* was fairly uniform with a small bias towards the *"top or right position"*, which is somewhat expected from predominantly right-handed users (see Figure 3.13b).



(a) (b)

Figure 3.13: **SemanticLock Data Analysis**: (a) The chart indicates the icon distribution is uniform *(standard deviation SD= 0.4)*. Users did not have any affinity to any particular password icon. **(b) Drag-To Positions**: This chart shows the analysis of the dragged Icon drag-to position on the stationary icon. Participants indicated an affinity for positioning password icons at the *"top"* position of the stationary password icon. Further analyses indicate that password icon positioning is uniformly distributed *(standard deviation SD= 0.2)*.

Password Icon pair distribution:

As each semantic password is composed of two or more sets of password icons, we pre-processed the collected data sets and decomposed semantic passwords that consist of more than two password icons into two pairs of password icons and performed frequency analysis on these password icon pairs. All pairs were roughly equi-likely (see Figure 3.14). Our analysis further shows a uniform distribution which indicates a strong password entropy.

3.4.4 Password Strength Evaluation

One objective for data collection during the Web study was to quantify and compare the results obtained from the PATTERN and SemanticLock system (see Figure 3.5). The metrics we obtained for pattern password evaluation were *Pattern-length*, *Stroke-length*, *Intersections*, *Start/End points* were similar to findings reported by [134, 7, 23, 49]. The data collected and our analysis was highly similar to those reported in past studies by [9, 23, 134, 16]. Implementing an accurate password strength comparison of the PATTERN and SemanticLock requires identifying metrics that are common to both systems or can be effectively generalized to serve our requirements. We determined that metrics such as

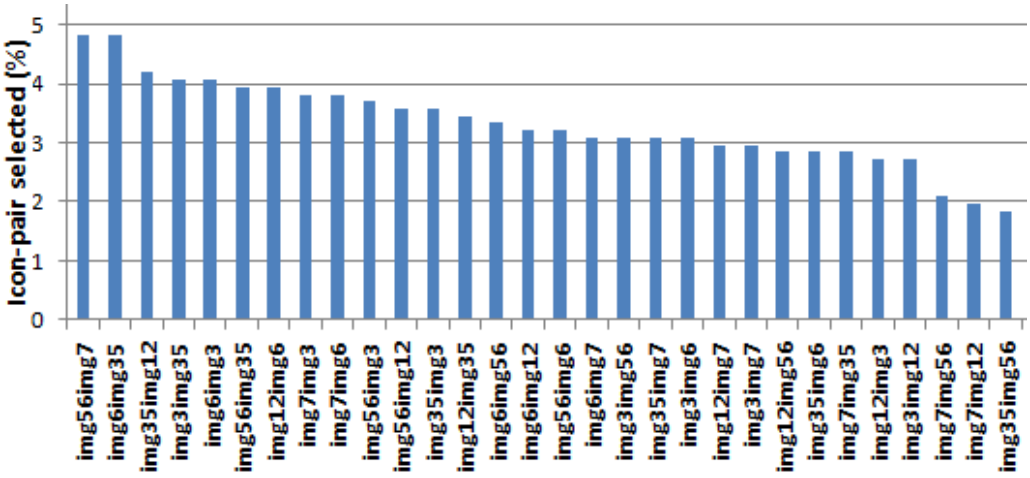


Figure 3.14: **Icon-Pair selection Analysis :** The distribution of "Icon-Pair" selection within the password icon data sets. The chart shows a "uniform" distribution, indicating a strong password entropy.

Start/End points and *guess-ability resistance* are best suited for our comparison needs.

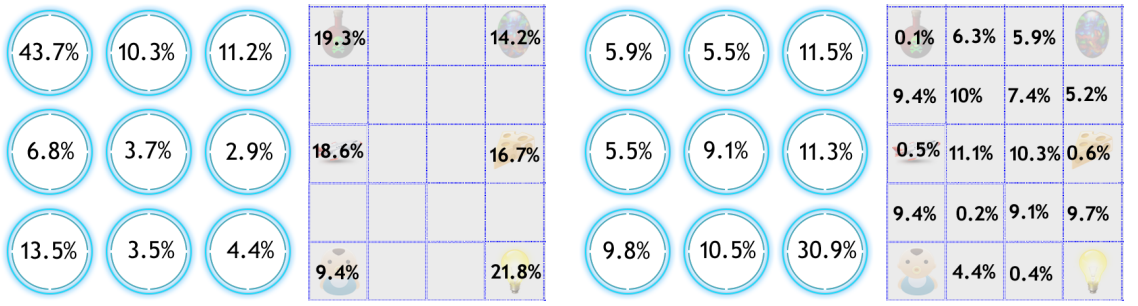
Table 3.2: Start/End point High values and Standard Deviation SD

System	StartPoint	StartPoint SD	EndPoint	EndPoint SD
PATTERN	43.7%	12.8	30.9%	7.8
SemanticLock	21.8%	**4.3**	11.1%	**4.1**

The table shows that SemanticLock performed better overall.

Password start and end Points

The uniform distribution of *start/end points* in a password system is an indication of high entropy and password strength [134, 7, 9]. Analysis of the Pattern passwords collected during the online study showed that 43.7% of our participants started their password from the top-leftmost node, making their starting points highly predictable (see Figure 3.15(a)). Unsurprisingly, participants chose the bottom right node as their end destination 30.9% of the time (see Figure 3.15(c)). These results are similar to findings observed by [134, 147, 23]. Analysis of the SemanticLock passwords collected during the online study shows the uniform distribution of start points (see Figure 3.15(b)), with the largest value



(a) Pattern Start points (b) SemanticLock Start points (c) Pattern End points (d) SemanticLock End points

Figure 3.15: **Start/End points comparison**: Percentage representation of the Start and End points.

of 21.8% located at the lower-rightmost cell, with a End point (see Figure 3.15(d)) of 11.1% located at the center of the grid (see Table 3.2). SemanticLock exhibited a lower level of bias and more uniform distribution of participant password Start and End points.

Password Guessability

The results of our guessing attack evaluation are displayed in Figure 3.16. In this figure, we depict guessing attack data for real user passwords, the PIN (4 digits) data was from a study by [15], and the PATTERN and SemanticLock data was collected during our web study. It can be seen that SemanticLock is more resistant to guessing attacks. For example, to compromise 20% *(i.e* α *= 0.2)* of the password space of the PATTERN authentication system, it requires 114 attempts, while SemanticLock requires 346 attempts and PIN required less than 50 attempts. Additionally, to compromise 50% *(i.e* α *= 0.5)* of PATTERN, it requires 438 attempts, while SemanticLock requires 2422 attempts and PIN required less than 100 attempts.

Our results are shown in Table 3.3 along with partial entropy estimates from other studies. We computed entropy estimates for α=10%, 20% and 50%, higher values of α for non-uniform distributions reflect a higher entropy factor. From Table 3.3, we note that SemanticLock has a better performance factor than all the *"practical"* $\text{PATTERN}_{(Tupsamudre,Aviv,Uellenbeck,Olade)}$ and RealUser PIN (4 digit) estimates, with its α values significantly higher than the password strength of a uniformly distributed 3-digit Random PIN.

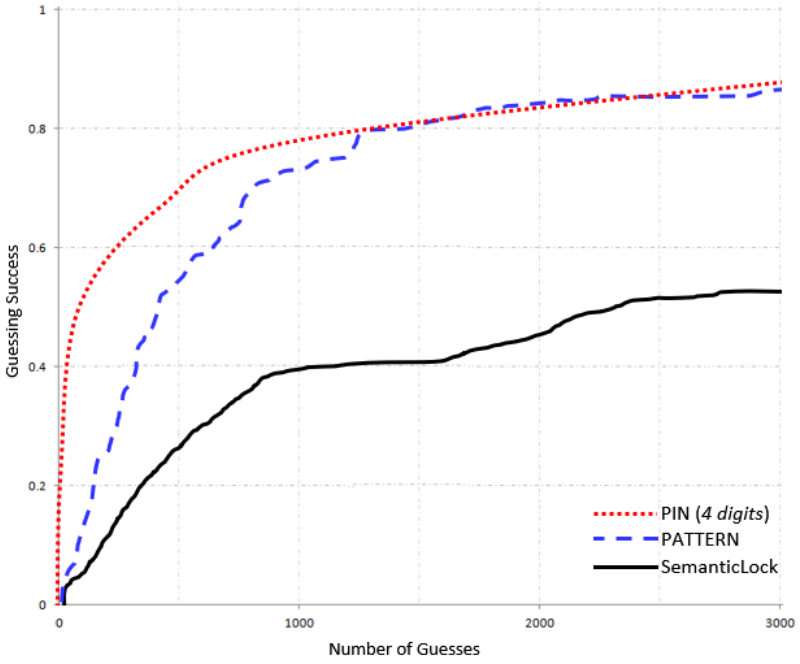


Figure 3.16: **Password Guessability Analysis :** Guessing entropy (α-*guesswork*) comparison of the guessing resistance of Random PIN (4 digits), PATTERN and SemanticLock. The graph of SemanticLock shows high resistance to guessing attacks.

Table 3.3: **Partial Guessing Entropy Comparison**: This chart compares partial entropy estimates of several distributions and different values for the (α-*guesswork*)

Distribution	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$
SemanticLock	**9.89**	**10.26**	**11.7**
PATTERN 3x3 (Olade)	7.10	7.86	9.98
RealUser PIN *(4 digits)* [58, 17, 15]	5.19	7.04	10.08
PATTERN 3x3 (Tupsamudre et.al) [133]	5.80	6.95	9.86
PATTERN 3x3 (Aviv et.al) [9]	6.59	6.99	8.93
PATTERN 3x3 (Uellenbeck et.al) [134]	8.72	9.10	10.90

3.4.5 Quantitative Results

Analysis of variance (ANOVA) is used to determine whether there are any statistically significant differences between the means of three or more independent groups or systems. ANOVA checks the impact of one or more factors by comparing the means of different samples. In this research, apart from using one-way and two-way ANOVA, we also per-

formed a Tukey Test, which is a single-step multiple comparison procedure to determine exactly where those differences lie.

Login Speed

The mean values of the login speed of each technique and other independent factors are shown in Table 3.4. The results show that the SemanticLock performed better than the other techniques across device form factors and postures. SemanticLock was superior in performance to PIN across all independent variables. There was a statistically significant difference between the techniques login speed as determined by the one-way ANOVA test ($F(4,535) = 170.44$, $p < .001$). A Tukey post hoc test revealed that SemanticLock (807.06 $\pm$ 167.23 ms, $p < .001$) was significantly faster than Pattern and PIN (both $p < .001$).

Table 3.4: Average login speed across posture and technique

Independent variables	Pattern	PIN	**SemanticLock**
Seated (Tablet)	785	1516	**590**
Seated (Phone)	825	1570	**652**
Walking Thumb	1135	1885	**853**
Walking Index	916	1395	**708**
Walking 2 Thumbs	945	1208	**768**
Walking-E Thumb	1175	1736	**917**
Walking-E Index	800	1474	**910**
Walking-E 2 Thumbs	873	1147	**655**

Note: *Walking-E* = Walking Encumbered

Differences across Device Form Factors

As stated earlier, we used two different types of device form-factors during the "seated" sessions (a Nexus 5 phone and a Google Pixel C tablet). Results of a two-way ANOVA test show that there was no significant effect of device form-factor ($F(1,530) = .003$, $p = .995$) on login speed across techniques. Furthermore there was no significant interaction effect between device form-factor and login technique ($F(4,530) = 1.208$, $p = .306$), (see Figure 3.17).

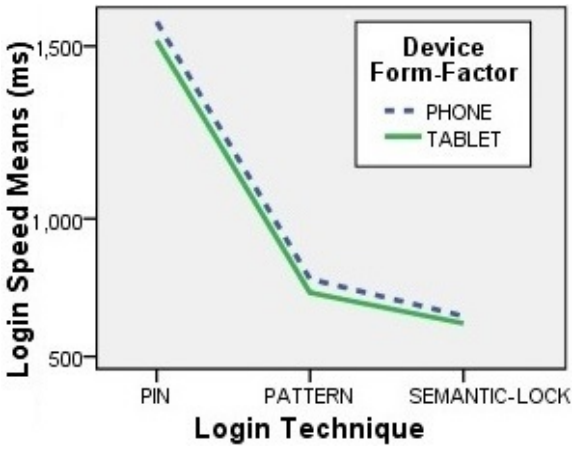


Figure 3.17: Login Speed compared on Device Form-factor indicates SemanticLock performed better on both device form factors.

Differences across Physical Postures

Our participants assumed three different physical postures (seated, walking and walking-encumbered). Results of a two-way ANOVA test show that there was no significant effect of posture ($F(2,1485) = 1.189$, $p = .305$) on login speed across Login techniques (see Figure 3.18). However, there was a significant interaction effect between physical posture and login technique ($F(8,1485) = 3.302$, $p = .001$), with participants having a faster speed using the SemanticLock method while walking encumbered.

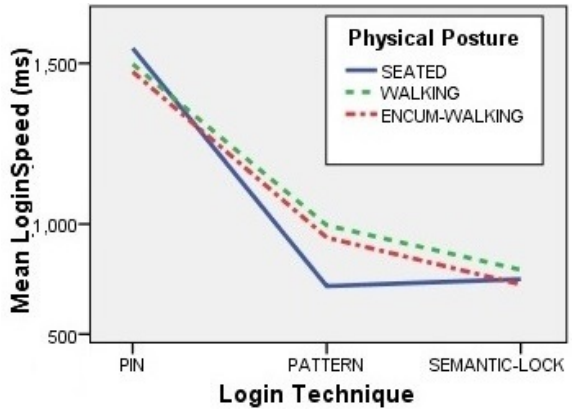


Figure 3.18: **Login Speed:** Login Speed compared on Physical Posture indicate that SemanticLock had a faster login speed when participants were walking unencumbered and walking encumbered.

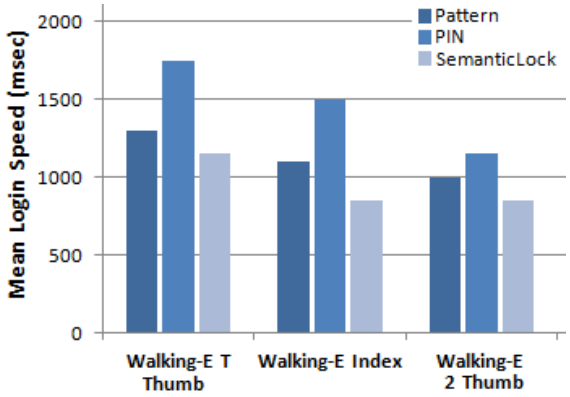


Figure 3.19: **Login Speed while Walking Encumbered:** Shows that SemanticLock performed better than the PIN and Pattern authentication systems while participants walked encumbered.

Further analysis of the data with the seated posture data excluded and using a two-way ANOVA test to examine the effect of walking posture (unencumbered or encumbered) and login technique on login speed show that there was no significant effect of walking posture ($F(1,950) = 1.757$, $p = .185$) on login speed across login techniques (see Figure 3.19). Furthermore, there was no significant interaction effect between walking posture and login technique ($F(4,950) = 1.660$, $p = .157$).

Differences across Input Hand Postures

Our participants while walking either unencumbered or encumbered assumed three different input hand postures (*OneHandThumb, TwoHands2Thumbs, OneHandOtherIndex*) during the testing of the Login Technique (see Figure 3.10). Results of a two-way ANOVA test conducted to examine the effect of Input Hand posture and login technique on login speed shows that there was a significant effect of Input Hand posture ($F(2,945) = 59.318$, $p < .001$) on login speed across login techniques (see Figure 3.20). Furthermore, there was a significant interaction effect between input hand posture and login technique ($F(8,945) = 2.973$, $p = .003$). A Tukey post hoc test revealed that the *TwoHand2Thumb* posture (1357 ms, $p < .001$) was statistically significantly faster than *OneHandThumb*, but there was no statistically significant difference between the *TwoHand2Thumb* and *OneHandOtherIndex* posture (1360 ms, $p = .965$).

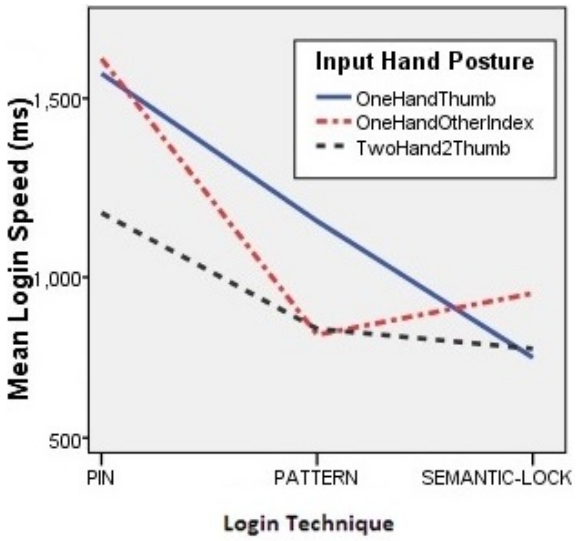


Figure 3.20: Login Speed based on Input Hand Posture for each Technique.

Pre-Login Delay Time

Our participants experience a time delay between when the trial started and when an initial action or interaction was made. This pre-login delay time gives an indication of familiarity, memorability or ease of use of the techniques. SemanticLock had the lowest pre-login delay time across all hand input postures (see Figure 3.21), the ANOVA test results showed a significant main effect for hand input posture, ($F(2,930) = 9.877$, $p < 0.05$) , where the *OneHandThumb* had a significantly lower pre-login time than the *Twohand2Thumb* but there was no significant difference with the *OneHandOtherIndex* ($p= 0.624$).

Error Rates

A two-way ANOVA test was conducted to examine the error rate for each technique. There was no significant effect of interaction by these independent variables on the error rate. Furthermore, the analysis showed that the error rate was lowest for all hand input postures when using SemanticLock and there was no significant difference in the error rate of the SemanticLock technique ($p = .925$). Additionally, results show that the PIN had the lowest error rates when walking unencumbered (see Figure 3.22).

It should be noted that data from the participants' "seated" sessions were excluded from this walking analysis. Error rates across all techniques indicate that participants in

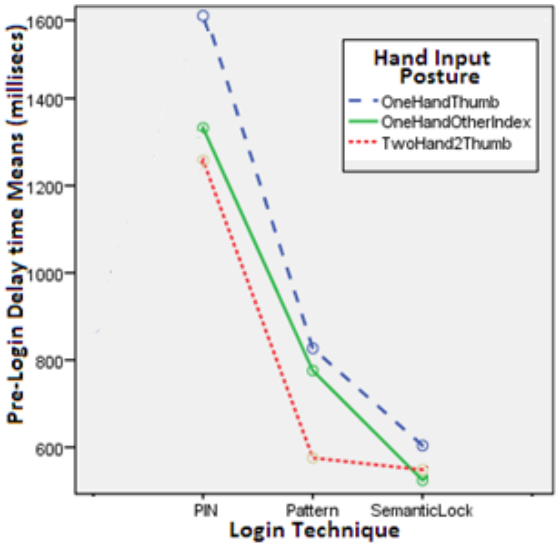


Figure 3.21: Pre-Login Delay Time based on Input Hand Posture for each Technique.

the seated position had the lowest error rates while the participants using two-handed both thumbs while walking unencumbered had the highest error rates (see Figure 3.29). Error rates classified by techniques show that Pattern (18%) had the highest error rates, followed by SemanticLock (7%), and PIN(3.5%) (see Figure 3.23).

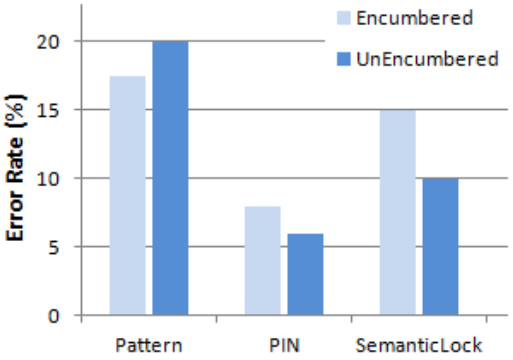


Figure 3.22: **Error Rates**: Error rate based on walking across all techniques.

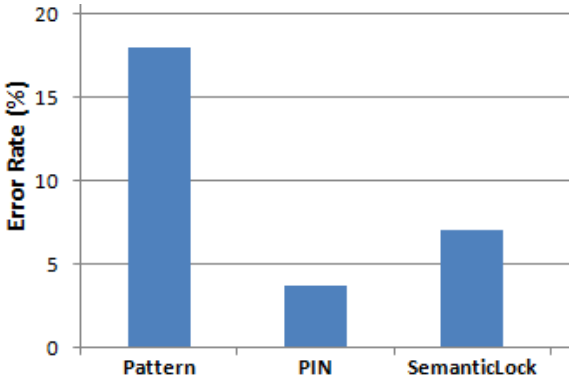


Figure 3.23: Error rates for each Technique

3.4.6 Qualitative Results

The results are based on a 5-point Likert scale questionnaire and subsequent user rankings of the three techniques. Each participant prior to the experiment answered an electronic pre-test survey which we used to obtain demographics, personal information, and mobile device user experience. The Likert scaled questions were answered after the trial of each technique to collect their subjective preferences. At the end of the trials, the user ranking of all techniques was collected (see Figure 3.24). The data we collected was analyzed using the Friedman test and we performed post hoc analysis with the Wilcoxon signed-rank test with Bonferroni correction (p= 0.05/3 = 0.017) of those that are statistically significant. In the questionnaire, we probed aspects of the users' experience with regards to the three login techniques, and their responses were analyzed.

Likeability

Post hoc analysis indicated that there was no significant difference in how well participants liked the techniques (see Figure 3.24).

Speed

Our participant's experience with each technique's speed shows there was a statistically significant perceived difference in speed depending on the technique ($\chi^{2(2)}$ = 18.321, p < 0.001) (see Figure 3.25). Post hoc analysis indicated that there were no significant differences of speed between PIN and Pattern trials (Z = -2.101, p = 0.036) or between

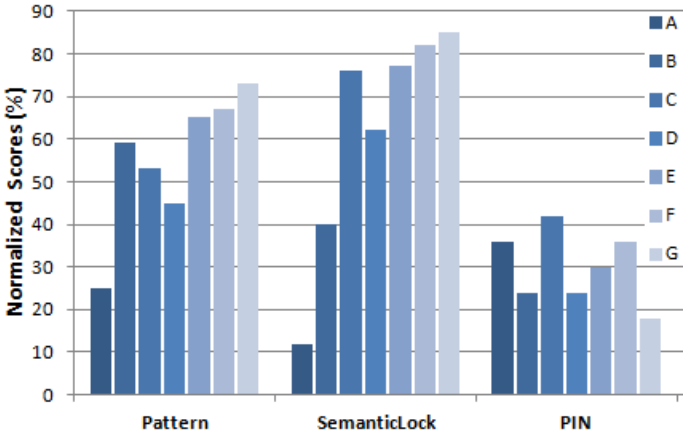


Figure 3.24: **User LIKERT ranking survey**: Our LIKERT based qualitative test indicates that the SemantickLock performed better with all the evaluated factors *(see legend A to G). [A: Hard to Recall, B: Best GUI , C: Easy to Recall , D: Use In Future , E: Liked the Most , F: Easy to Use , G: Faster Login]*

PIN and SemanticLock trials (Z = -1.560, p = 0.119). However, there was a significant difference in speed between Pattern and SemanticLock trials (Z = -3.573, $p < 0.001$), with SemanticLock perceived to be significantly faster.

Usability

There was a significant difference in perceived ease of use of the technique ($\chi^{2(2)} = 14.22$, p = 0.001). Post hoc analysis indicated that there were no significant differences between the PIN and Pattern (Z = -1.672, p = 0.94) or between the PIN and SemanticLock (Z = -1.628, p = 0.103) (see Figure 3.26). However, there was a significant increase in perceived ease of use between Pattern and SemanticLock (Z = -3.140, p = 0.002).

Positive Feedback

Participant‘s experience with the feedback for each technique also showed that there was a significant difference ($\chi^{2(2)} = 17.179$, $p < 0.001$) (see Figure 3.27). There were significant differences between Pattern and SemanticLock as well as SemanticLock and PIN; SemanticLock was ranked favorably in both cases.

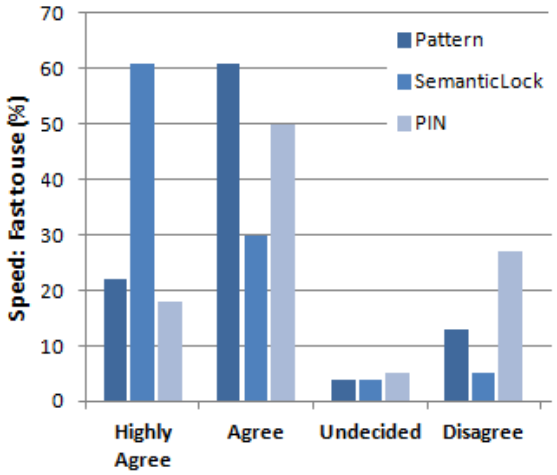


Figure 3.25: **Perceived Login Speed:** A comparison of the users' perceived login speed for each technique.

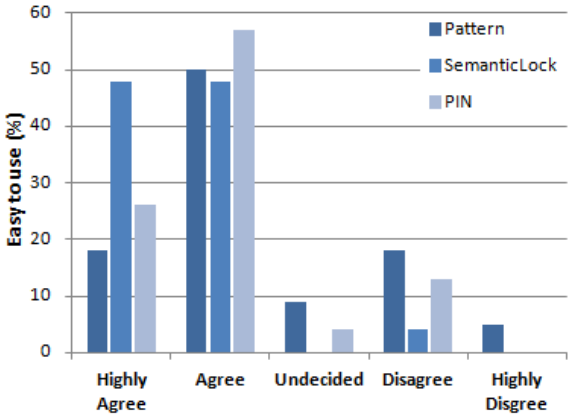


Figure 3.26: **Easy to use:** Results also indicates that 48% of participants believe that SemanticLock was "easy to use".

Error Recovery

There was a significant difference in error recovery based on technique ($\chi^{2(2)} = 12.667$, p = 0.002). Significant differences were found between Pattern and SemanticLock as well as PIN and SemanticLock. In both cases, Pattern and PIN were ranked favorably in regard to ease of error recovery. There was no significant difference in how participants liked interacting with the techniques (see Figure 3.28).

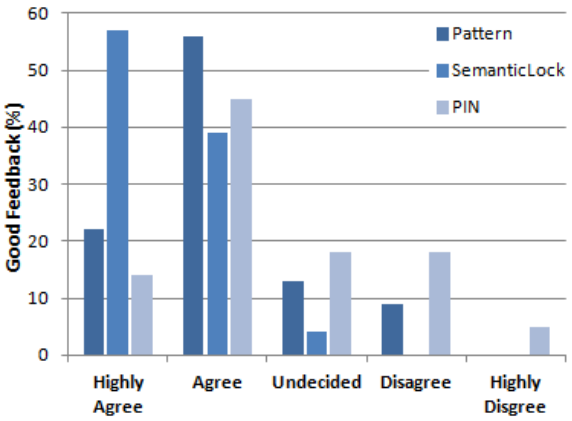


Figure 3.27: **Positive Feedback:** Results also indicates that 57% had a positive opinion of SemanticLock.

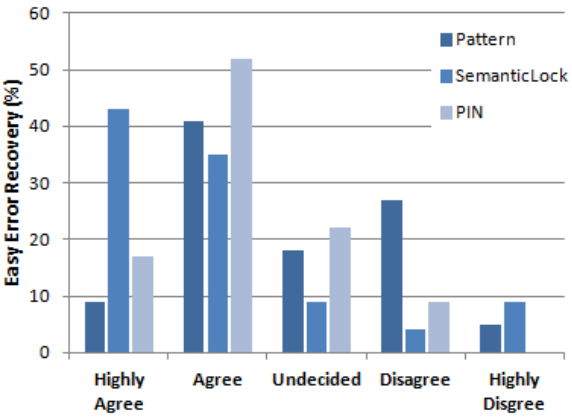


Figure 3.28: **Error Recovery :** Results also indicates that 43% observed easy error recovery when using SemanticLock.

3.5 Discussion

Data analysis indicates that SemanticLock clearly has a stronger practical password strength than the PATTERN or PIN authentication system. Results from section 3.4.1 show that SemanticLock has little or no password Start/End point bias (see Figure 3.15). Furthermore, evaluations performed using partial guessing entropy shows that the practical entropy of SemanticLock is closer to the security offered by a uniformly distributed Random 4-digit PIN and outperformed all the practical strength of the PATTERN authentication system

examined in this thesis (see Table 3.3).

3.5.1 Login Speed

Our participants performed significantly better using the SemanticLock. We believe the two simple swipe movements to create the password gave our technique the advantage of a faster login speed. The data from the quantitative and qualitative (see Figure 3.25) analysis supports our observations. We initially expected that the Pattern authentication system would be faster due to the participant‘s familiarity but this was not the case.

3.5.2 Error rates

Our participants experienced the lowest error rate when seated (see Figure 3.29) and using their preferred Hand Input posture. Interestingly, we also discovered that during the walking session PIN had the lowest error rate across all techniques (see Figure 3.22). Participants ranked the techniques based on how easy it was to recover from errors in this order: Pattern (9%), PIN (17%), and SemanticLock (43%). Meaning that SemanticLock was far easier to recover from its errors. It would appear that the combination of short continuous/discrete movements allow users to recover from errors better.

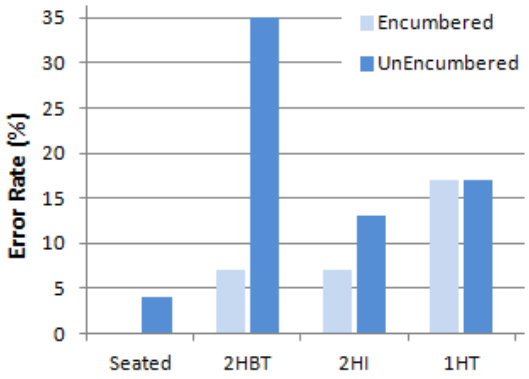


Figure 3.29: **Error Rates**: Error Rate based across all techniques by posture. Login activities performed while seated had the lowest error rate across all techniques.

3.5.3 Memorability Test

Our participants displayed varying levels of difficulty in recalling their passwords. Our analysis based on the data is shown in Figure 3.30. The memorability ratio of the Seman-

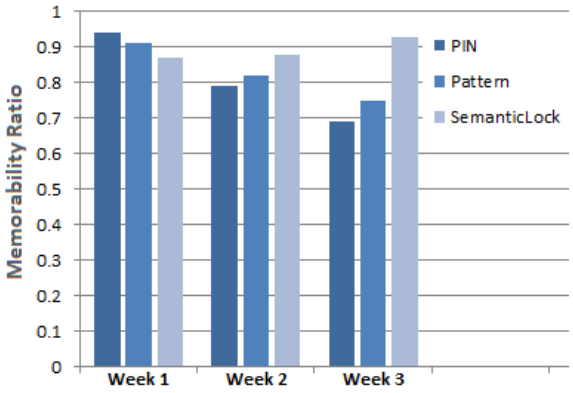


Figure 3.30: **Password Memorability:** Results also indicate a steady increase in memorability when using SemanticLock.

ticLock steadily increased every week. This is an indication that the Semantic-lock was more memorable to the participants.

3.6 Conclusion

In this study, we have explored a novel and new screen lock concept based on semantic constructs. We used novel aspects such as; set of graphical images as password tokens, which are intended to enhance password memorability. The user is able to create a password using quick actions of dragging and re-positioning image tokens into their respective positions via a combination of discrete and short continuous actions on the touchscreen. The large number of possible semantic constructs derived from the (re)positioning of the image tokens and the varieties of images to choose from give our method a theoretically large password space and the current selection of images gives it a large practical password space, and these images can be changed by users to make password tokens even more customisable and memorable. We believe that SemanticLock‘s performances will improve when users have more practice and familiarity with it. In regards to generalization, our sample population represents the most common demography of mobile device users and should be able to generalize to other populations. The results of a three-week mobile device user study with participants using SemanticLock plus PIN and PATTERN show that SemanticLock generally has superior performance compared to PATTERN and PIN authentication techniques on key metrics such as login speed, memorability, user accep-

tance, usability, and likeability. All in all, SemanticLock represents a simple, easy-to-use, and usable authentication method for mobile devices and is a good alternative to other common methods. We observed the below key lessons :

- Graphical authentication systems based on discrete and continuous movements outperform other authentication systems. The potential of SemanticLock to be faster than the PATTERN is attributed to these dual movement properties.
- Authentication systems based on core graphical tokens with mnemonic properties result in higher memorability values.
- Error recovery is strongly influenced by system design. We determined that graphical user interactivity and user familiarity greatly reduces the error rates.
- The SemanticLock had the shortest pre-login delay time, which means that the participants found it easier to recall their password faster than with other techniques, therefore indicating better memorability factors.
- The type of device used by the participants (i.e. phone or tablet) had no effect on their performance.
- SemanticLock performed excellently during the walking test. The results for both walking encumbered and unencumbered provided a good indication of its potential use under these scenarios.

Chapter 4

Exploring the Vulnerabilities and Advantages of PATTERN Authentication in VR

4.1 Introduction

In the previous chapter, we examined a new graphical authentication system that used semantic constructs, that were derived from the repositioning icon tokens. After a 3 week study and final analysis, our participants found SemanticLock more usable and secure than the current mainstream PATTERN and PIN mobile device authentication system. In this chapter, we explore a new mobile device environment, examining the performance and interaction complexities of the PATTERN mobile device authentication system within the virtual reality ecosystem. This enables us to examine the research gaps for our upcoming experiments.

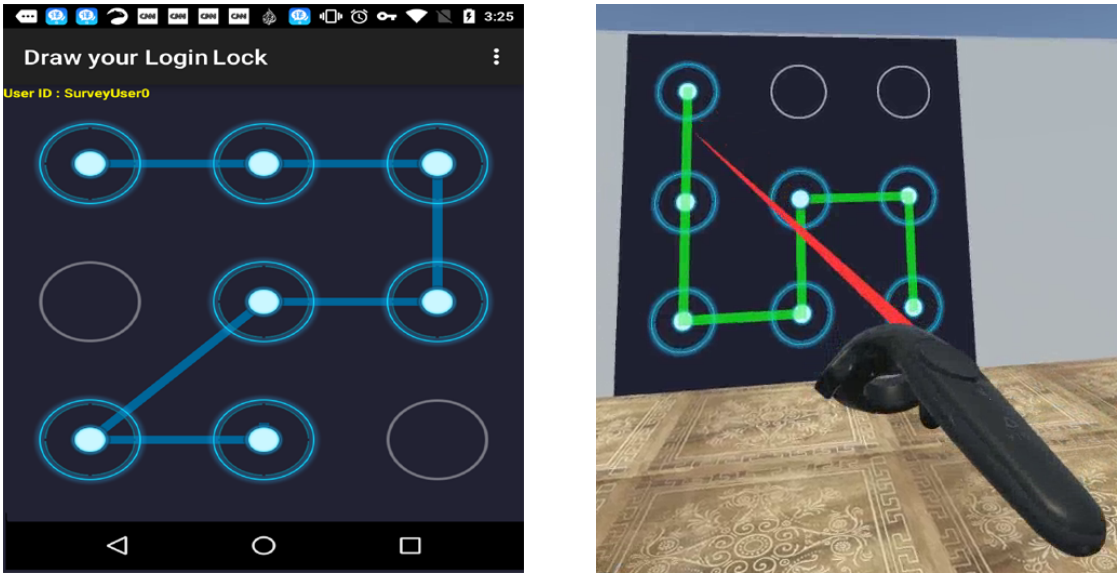
Virtual Reality (VR) has quickly gained a large user base as the technology becomes cheaper, mainstream and more applications exist for this new environment. We observed its usage in education [24], medical [46], shopping [117], advertisement [37] and manufacturing [12] sectors. Some innovators and concept developers in the industry see VR as an evolution of the popular mobile device market and rely on existing mobile device consumers in that sector to promote and sustain the growth of this new trend [151, 102]. Global online retailers and e-commerce platforms, such as Amazon and Alibaba have introduced virtual

malls where VR enabled clients can walk through the shop and virtually interact with the products on sale. Virtual reality is here to stay and as the application of virtual reality continues to expand, the issue of user security and the lack of a standard authentication becomes increasingly apparent [36]. We believe that VR and mobile devices, especially smartphones and tablets are intrinsically linked in terms of usage, while other researchers [151, 102] are exploring the development of new authentication technologies for the VR environment such as biometrics [109, 62] and kinesiology [73, 111, 55]. We are looking at porting an existing mobile device authentication system and observing how they perform in this new environment and this has the advantage of pre-existing popularity and familiarity. We are vividly aware of the security challenges plaguing the mobile device authentication systems as large body of research [49, 60, 138, 1, 84, 7, 152] exist in that field and we wish to explore the possible fallacies and advantages that a VR version of these authentications may have; considering the fact that VR users are a large subset of existing mobile device users. Our research focuses on examining the performance and usability factors of the popular mobile device authentication system known as PATTERN lock within the VR environment. This system was made popular by the Android smartphone market and it is now practically the defacto authentication system on every mobile device.

The PATTERN authentication system is a grid-like display of nodes (see Figure 4.1) whose password pattern is selected by continuous finger or pointer movement across the screen to connect the password nodes. PATTERN has been plagued by numerous usage and security issues [152, 134, 49, 140] in the mobile device usage ecosystem, and one of the most prominent security weakness is Shoulder-surfing. We argue that the VR version of PATTERN would be highly resistant to shoulder-surfing and will also perform comparatively well in other usage aspects such as speed, error-recovery, and high entropy.

4.2 Threat Model

Our threat model is designed to evaluate the possible vulnerabilities of our VR PATTERN systems and it is based on previous studies. In our simulated attack, we define three types of attackers. Type A attacker has no prior observation of the user and the attack is based primarily on brute-force measures and social engineering [130, 6]. Type B attacker is more effective; this attacker has observed the valid user on several occasions during an authentication session or has access to video footage of the entire login session from multiple strategic camera viewpoints. The Type C attacker is the most promising because



(a) SmartPhone PATTERN (b) VR PATTERN

Figure 4.1: **Prominent mobile device authentication systems**: The PATTERN authentication system is popular with (a) mobile devices that have GUI touchscreen-based systems. (b) Shows the VR PATTERN ported to the Virtual reality environment.

this attacker is also actually the valid user who has forgotten the actual password due to long periods of not using the password. This attacker is allowed to watch previous video footage of their own authentication process. This type of White-box penetration testing allows our study to get a better perspective of the level of Shoulder-Surfing [148] resistance our system possesses.

4.3 Methodology

We utilized three environments and two different sets of participants for data collection during this study. A detailed discussion of our study follows.

4.3.1 Participant recruitment and ethical concerns

Because our study utilizes human subjects, it was reviewed and approved by our University Research Ethics committee. One concern raised was whether or not participants would inadvertently reveal their personal passwords. To prevent this, a text was added in the

instructions of each experiment specifically warning participants not to use any current or past personal password as part of their responses. Participants for all experiments were volunteers, recruited via a university-wide e-mail. Participants were primarily students, but also included some staff members. All participants were daily mobile device users. Participants in the web survey portion of our study were not compensated, due to a large number of participants and the relatively short duration of their participation. Volunteers for the longer-term memorability and usability studies were compensated with coffee shop gift cards worth between 5 and 30 US dollars, depending on the duration of participation.

4.3.2 Experimental Design

Our goal was to compare the performance metrics of the mobile phone version of the PATTERN authentication system to those of the virtual reality version of the authentication system. To do this, we followed a within-participants design. Below are the variables we tracked:

The independent variables are

- **Device Form-Factor**
    1. Mobile Device
    2. Virtual Reality (VR)
- **Interaction Methods**
    1. Mobile device : Touchscreen
    2. VR Hand-Held-Controller (HHC)
    3. VR Head-Mounted-Display (HMD)
    4. VR LeapMotion
    5. VR Eye-Tracking

The dependent variables are

- Login Speed
- Pre-Login Delay Time
- Error Rate
- User usability and acceptance
- Shoulder-surfing resistance

Study Outline

We utilized three studies for data collection in an attempt to expose and collect the data we need for our planned evaluation and comparison. The studies conducted were a web-based study, a mobile study, and a virtual reality environment study.

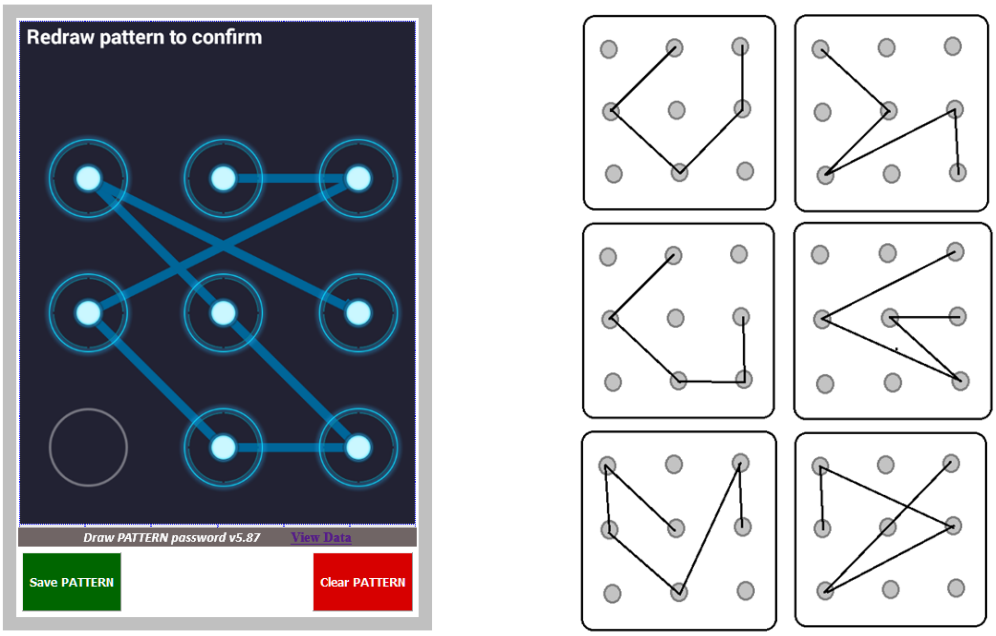
Web Study: An Internet-based study, where a large number of participants were allowed to create a series of PATTERN passwords via a web-based version of the PATTERN system (see Figure 4.2a). The collected passwords were used for analysis (see Section 4.3.4).

Mobile Device Study: A mobile device study, using Android-based mobile phones (see Figure 4.1a). Participants were tasked with creating and using the PATTERN password over a period of time. Data collection and real-time participant survey was done via the custom-built android PATTERN authentication system (see Section 4.3.5).

Virtual Reality Study: This study involved creating a virtual reality version of the PATTERN authentication system (see Figure 4.1b). Participants interacted, using 4 different interaction methods, and created passwords while various metrics were tracked and logged for analysis (see Section 4.3.5). We also made a video recording of these sessions from 3 different points of view.

User Interaction Methods

Participants used five different methods to interact with the PATTERN authentication system. The mobile device interaction is solely via the touch-screen, whereas the virtual



(a) PATTERN Web Study Interface (b) 6 PATTERN Passwords

Figure 4.2: **Web Study**: The PATTERN Web Study presented a Web version of the PATTERN interface (a) to participants who were asked to create random passwords. (b) From the numerous passwords, we selected 6 passwords that were complex and uncommon.

reality environment PATTERN authentication system allowed us to use four VR interaction methods as explained below :

Touch Screen: This is a property of mobile device screens that are able to respond to touch. The participants use their fingers to touch and drag GUI objects around the mobile device touchscreen, thus performing an interaction with the system.

Hand-Held-Controller (HHC): The HHC is a physical interactive device (see Figure 4.3a) held by the participant in a virtual reality environment. This device has a series of buttons and also provides to the VR system important data such as the position, rotation, and speed of the participant's hand. Additionally, when represented in the VR environment it can project a virtual laser beam of light to act as a *pointer* that the participants can use to select and manipulate objects within the VR space.

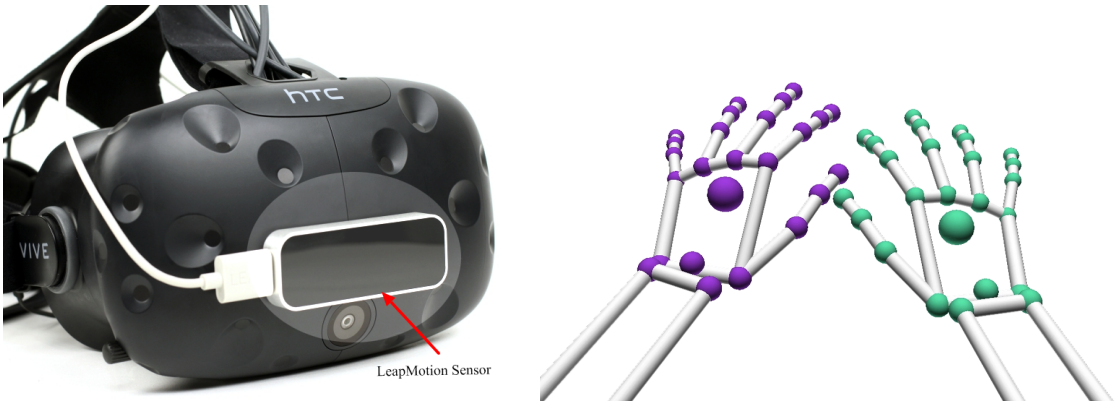
(a) VR Hand Controller (b) EyeTracking HMD

Figure 4.3: **Prominent mobile device authentication systems**: (a) Participants use the HHC to interact with VR objects with six degree of freedom (6-DOF).
(b) Interior view of a HMD device fitted with Eye-tracking hardware .

Head-Mounted-Display (HMD): The HMD, is part of the VR headset unit (see Figure 4.4a) and uses inertial motion sensors to estimate the participant‘s head position and rotation in world-space, these sensors obtain data concerning the HMD and constantly update the VR visual scene according to head movements. The HMD presents virtual reality visuals to represent these changes and transitions of the participants‘ head. The HMD allows us to extract the positional coordinates, rotational, acceleration and velocity data of the participants during our experiment.

LeapMotion: LeapMotion [65] is a hand tracking infra-red based system (see Figure 4.4a), that tracks the hands of the user and feeds the data into the VR systems where a digital representation of the hand (see Figure 4.4b) is rendered. The digital representation can be used to interact with other objects within the Virtual reality environment.

Eye-Tracking: Eye-tracking hardware, called aGlass [3], was installed inside the HMD to track the participants‘ gaze as they performed their task. We track the positional coordinates (x,y) or direction where the participant is looking at within the virtual scene. We determined based on the gaze period if the participant was initiating a selection and drawing a PATTERN password. The eye tracker was calibrated with a 9-point accuracy method (see Figure 4.3b).



(a) LeapMotion sensor (b) Virtual Hands

Figure 4.4: **VR LeapMotion Hand Tracking**: (a) External view of HMD with a LeapMotion sensor attached to the front *(silver square sensor on front panel)*. (b) Digital representation of user's hands in VR based on actual hands.

4.3.3 Apparatus

Study Software

In our study, we developed exact functional replicas of the PATTERN software (see Figure 4.1 and 4.2a) for each platform to be able to integrate data collection functions into the software system process flow. We made great efforts to ensure the PATTERN software was visually and functionally similar regardless of the implementation platform.

Web Interface Software: We implemented the PATTERN web-based interface (see Figure 4.2a) using HTML5, CSS, PHP, and MySQL database back-end technologies. This allowed us to implement graphical line drawing and icon high-light functions that are common on touch-screen based devices. Data collected was saved in the database.

Mobile device Software: We created the mobile device system (see Figure 4.1a) with Android Studio on a Windows 10 PC *(Intel Core i7-6700, 128GB RAM, NVIDIA GeForce 1080)*. Data collected on the mobile devices were stored as a text file on the device.

Virtual Reality Software: We created a VR environment (see Figure 4.1b), with Unity3D and C# on a Windows 10 PC *(Intel Core i7-6700, 128GB RAM, NVIDIA GeForce 1080)* to assist in the collection of our experimental data. Data collected was saved as a CVS on

the PC running the VR environment.

Study Hardware

Touchscreen Mobile: Mobile devices are available in numerous dimensions. We performed our study with a 5.2" LG Nexus 5X phone [67].

Virtual Reality Hardware: The Virtual Reality system we used for our study is the HTC VIVE hardware [137] with standard handheld controllers (see Figure 4.3a). Third-party add-on hardware such as aGlass [3] for Eye Tracking (see Figure 4.3b) and Leap-Motion Hand tracking [65] (see Figure 4.4) were also used to provide additional tracking information, thus creating a better realistically immersing VR experience.

4.3.4 Web-based Study

We presented the participants with a 3x3 PATTERN web-interface (see Figure 4.2a) and requested that they create 10 unique passwords that have more than 3 nodes. Although web-based experiments are harder to control than laboratory or supervised field studies, this channel of data collection meets our requirements, offers numerous advantages and allowed us to collect large amounts of data from our participants at various locations. Each participant was tracked via their device Internet Protocol (IP) address and their chosen PATTERN patterns were logged in a database.

Goals

Our primary goal was to quantify the effect of a participant's choice on the security of passwords chosen. Every authentication scheme has entropy and the strength of such entropy is determined by the probability distribution associated with the password space. Ideally, this distribution is approximately uniform. We selected from the provided passwords, six PATTERN patterns that we decided were well distributed across the password nodes (see Figure 4.2b) to be used in the Mobile Device and Virtual Reality study.

(a) VR:LeapMotion (b) VR:HHC (c) VR:HMD

Figure 4.5: Participants using various VR interaction techniques.

Participants

We created awareness about the Web study via social media and the university mailing list. A tutorial video was made available on the website so participants could watch and learn how to create PATTERN password patterns. We had no input in selecting the participants, we did not collect any demographic information about these participants, but we ensured their IP was unique.

4.3.5 Mobile Device and Virtual Reality (VR) Study

We developed a mobile device version (see Figure 4.1a) of the PATTERN interface that was used during our web-based study (see Figure 4.2a). This mobile device authentication system will be our baseline or control for this study due to the popularity and large body of research literature [134, 7, 28, 22, 25, 49, 152] about its performance. It is important to note that due to the peculiarity of this VR environment (see Figure 4.1b) we explored 4 different methods of user interactions (see Section 4.3.2). Each participant used 5 different interaction techniques (see Section 4.3.2) and completed 3 PATTERN login trials per interaction technique (see Figure 4.5). During the VR session, the participants' physical Login movements or actions were recorded with a video camera. We captured their actions (see Figure 4.6) from 3 different points of view (Front, Top and Side). These recordings will be used to analyze the level of resistance that virtual reality (VR) has against Shoulder-surfing. Lastly, we provided a paper-based survey questionnaire to collect qualitative feedback from our participants in a uniform and consistent way.

Goals

Our objectives during the study, which involved participants, was to collect both qualitative and quantitative data which would provide insight into our participant's perception of the likeability, usability, memorability and login speed of both types of the PATTERN authentication system (see Figure 4.1). During the testing, a participant's activities such as touches, password tokens, strokes, pauses, timings, aborts, and errors were logged for further analysis.

Participants

We recruited 15 participants from a local university and 51% of the participants were between the ages of 17 to 27 and all our participants were right-handed. All were active users of mobile phones and 60% had experience with Virtual Reality devices. 70% of them used a phone with a fingerprint sensor, while 10% used the PIN, and 20% used PATTERN.

Task and Procedures

Our first step was to inform the participants about the confidentiality of their supplied information and to explain the purpose of the project and the tasks they would need to do. We required that everyone start with the mobile device environment, then conclude with the virtual reality environment. We provided a five-minute training video to each participant that depicts the usage of PATTERN in the mobile device and virtual reality environment. We calibrated each participant‘s eyes for the aGlass EyeTracker software and created a profile for each person and also explained the usage constraints of the LeapMotion device, then we allowed participants to practice with the Virtual Reality equipment and alerted them to the possibility of motion sickness while in the virtual reality environment.

Week 1 (First Phase): We allowed each participant to choose a PATTERN password from our supplied list (See Figure 4.2). During the experiment, the participants are required to enter this selected password 3 times during the session. If the participant entered the wrong password, the application alerted them to enter the correct password again. The experiment finished with a Likert questionnaire that collected qualitative data about the participants' perceived *usability, error-handling, security, and likeability.* The average time the participants used to complete the mobile device experiment was 2 minutes while the VR experiments took about 14 minutes.

Week 3 (Second Phase): In the second phase, i.e. 15 days after the first phase, we explored the effects of shoulder-surfing within the VR environment. In this session we used 12 participants as "Attackers", we selected 2 persons who were not involved previously with the study as *Type A and B* attackers, and used 8 persons from week 1 (see section 4.3.5) of our project who we confirmed were unable to remember their week 1 Login passwords as *Type C* attackers. *Type A* attackers were not allowed to view the videos, while *Type B* attackers as defined earlier in Section 4.2 of this thesis, viewed the videos and wrote down 3 possible passwords based on their visual evaluation of the participants' actions. *Type C* attackers viewed only their own videos. The outcome of this session is analyzed in Section 4.5.1.

4.4 Data Collection and Measurement

A description of the data that we collected and its relevance to the study.

4.4.1 Pre-Login Delay time

Pre-login delay is the elapsed time between when the participant indicated that they were ready to start unlocking the device and the actual time they entered the password. This data provides a view into evaluating the memorability and usability of the system. Studies by Stobert et al. [127, 144] defined a direct relationship between memorability and pre-login delay time. We analyze this data to quantify the level of memorability and usability experienced by the participants.

4.4.2 Login Speed

The time period used to complete each trial of the login process for an interaction technique was recorded. This measurement only recorded successful trials; failed trials were recorded as singular failure events. Login speed was tracked from the moment a participant starts password token entry until the entry was completed successfully.

4.4.3 Error Rate

The error rate was measured as a percentage of failed login attempts to the total number of attempts required to complete the technique's session. The number of failed login attempts during a trial did not affect the number of trials that constituted a complete session.

4.4.4 Shoulder-surfing Attack Evaluation

Shoulder-surfing is a known weakness of PATTERN on mobile devices [152, 148, 134, 22]. We setup three high-resolution cameras to record the physical actions of the participants. These cameras captured the *Front, Top and Side* views of participants while ensuring that their entire body was visible as they performed both the mobile device and VR sessions (see Figure 4.6). The video feed was multiplexed into a single video allowing the 'attackers' to observe the participants simultaneously from all views.

Figure 4.6: Shoulder-surfing evaluation was performed by recording the participants' Login actions via 3 video cameras and having future 'attackers' view these recordings in an attempt to guess the passwords.

4.4.5 Subjective Data

We collected *pre-test*, *in-test*, and *post-test* surveys via an electronic questionnaire for the mobile phone study, while the VR questionnaire was paper-based. The questions focused on ease of use, perception of speed, the likelihood of adoption, error recovery, and interface usability.

4.5 Results

We present the results of our study in both *quantitative* and *qualitative* formats. This analysis is based on the raw numerical data and subjective data we collected from the

participants.

4.5.1 Quantitative Results

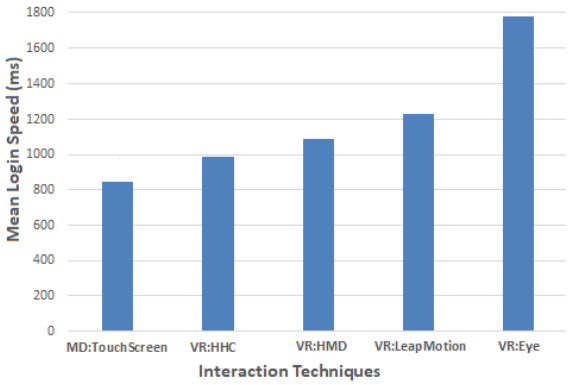


Figure 4.7: **Login Speed:** Mean Login speed based on interaction techniques. The mobile device Touchscreen has the lowest login time.

Login Speed

The Login speed data from the study indicates that *MD:Touchscreen* login speed was faster than any of the other VR interaction technique login speed. The mean values of the login speed of each interaction technique are shown in Figure 4.7. The one-way ANOVA test ($F(4,461) = 120.19$, $p < .031$) indicates statistical differences between the interaction techniques. A Tukey post hoc test revealed that *MD:Touchscreen* login speed (913.04 ± 172.53 ms, $p < .001$) was significantly faster than all VR interaction techniques, and there was also statistically significant difference between the *VR:HHC* and the *VR:Eye* but there was no statistically significant difference between the *VR:HHC* and *VR:HMD* interaction techniques (960 ms, $p = .965$) or the *VR:LeapMotion*.

Pre-Login Delay Time

Our participants experience a time delay between when the trial started and when an initial action or interaction was made. This pre-login delay time gives an indication of familiarity or ease of use of these interaction techniques. Our analysis indicates that the *MD:Touchscreen* has the lowest Pre-Login Delay time and the VR:Eye interaction

technique has the highest time (see Figure 4.8). This is understandable since the virtual reality environment was novel to most participants.

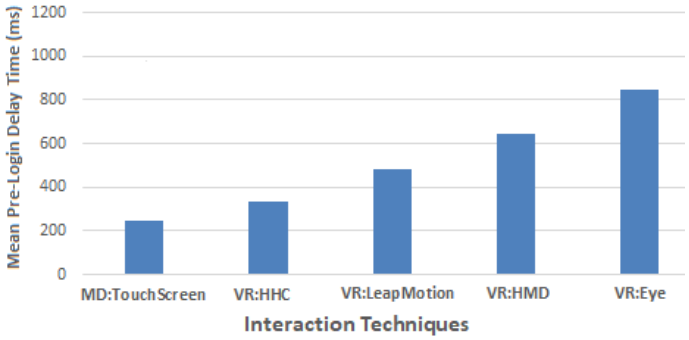


Figure 4.8: **PreLogin Delay time:** The PreLogin Delay Time is an indication of ease of use or familiarity of the interaction techniques

Shoulder-surfing Attack results

Our 12 attackers consist of 2 Type-A attackers and 2 Type-B attackers. These 4 attackers were allowed to watch the video recording of all the 15 participants sessions. While the 8 Type-C attackers who were former participants that forgot their passwords were allowed to watch their previous login sessions. The 3 passwords could be of the *3-Node match*, *4-Node match* or *full match*. We observed that 97% of the sessions used a 5-Node password. The results indicate that the VR environment is highly resistant to shoulder-surfing with the *Type C* attacker achieving a *Full Match* of 36% while *Type B* attacker and *Type A* attackers have a 20% and 3% success rate respectively. We allowed the Type B and C attackers to view the video recording of the mobile phone study sessions and the results were 100% Full Match for all sessions, this supports the fact that mobile devices have little or no resistance to well-implemented forms of shoulder-surfing. (see Figure 4.9).

Error Rates

Error rates classified by interaction techniques are an indication of the usability level of the interaction techniques. As mentioned earlier, most participants are new to the VR environment, but we notice that the error rates of the *VR:Eye* and *VR:HMD* were very high. Some system errors due to the *VR:Eye* hardware malfunctions were accounted and adjusted for. A two-way ANOVA test was conducted to examine the error rate for each technique. There

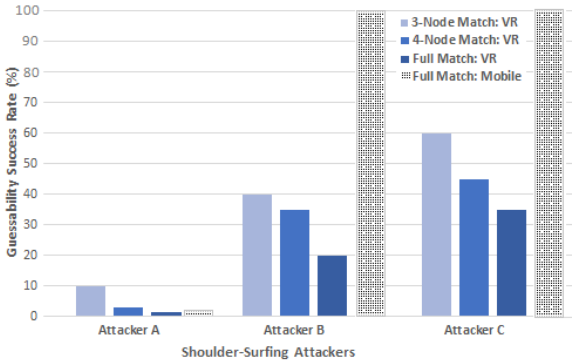


Figure 4.9: **Shoulder-Surfing Attack:** Results from the Shoulder-surfing attack process. We defined the attackers and provided different knowledge and access to recorded videos, then allowed these attackers to guess the PATTERN passwords that they observed.

was no significant effect of interaction by these independent variables on the error rate. Furthermore, the analysis showed that the error rate was lowest for *MD:Touchscreen* and there was a significant difference in the error rate of the *MD:Touchscreen* technique across all interaction techniques (p = .001).

4.5.2 Qualitative Results

The results are based on a 5-point Likert scale questionnaire and subsequent user rankings of the five interaction techniques. Each participant prior to the experiment answered a pre-test survey which we used to obtain demographics, personal information, and mobile device/VR usage experience. The Likert scaled questions were answered after the trial of each technique to collect their subjective preferences. The data we collected was analyzed using the Friedman test and we performed posthoc analysis with Wilcoxon signed-rank test with Bonferroni correction (p= $0.05/3 = 0.017$) of those that are statistically significant. In the questionnaire, we probed aspects of the users' experience with the five login interaction techniques.

Speed

Our participants' experience with each interaction technique's speed shows there was a statistically significant perceived difference in speed depending on the technique ($\chi^{2(2)} = 18.321$, $p < 0.001$) (see Figure 4.10). Post hoc analysis indicated that there were no

significant differences between *VR:HHC* and *VR:HMD* trials (Z = -2.101, p = 0.036) or between *VR:HMD* and *VR:LeapMotion* trials (Z = -1.560, p = 0.119). However, there was a significant difference in speed between *MD:Touchscreen* and *VR:HHC* trials (Z = -3.573, $p < 0.001$).

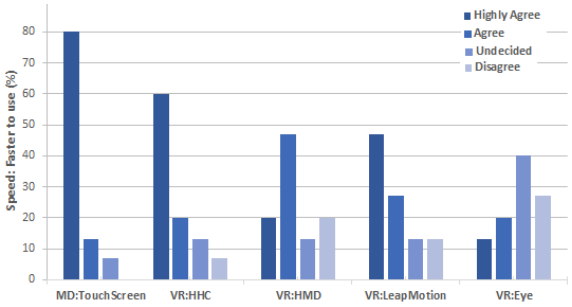


Figure 4.10: **Perceived Login Speed:** A comparison of the users' perceived speed for each interaction technique.

Likeability

Post hoc analysis indicated that there was no significant difference in how well participants liked the techniques.

Usability

There was a significant difference in perceived ease of use of technique ($\chi^{2(2)} = 14.22$, p = 0.001). Post hoc analysis indicated that there were no significant differences between the *MD:Touchscreen* and *VR:HHC* (Z = -1.672, p = 0.94) or between the *VR:HHC* and *VR:LeapMotion* (Z = -1.628, p = 0.103) (see Figure 4.11). However, there was a significant increase in perceived ease of use between *VR:HHC* and *VR:Eye* (Z = -3.140, p = 0.002).

Error Recovery

There was a significant difference in error recovery based on the interaction technique ($\chi^{2(2)} = 12.667$, p = 0.002). Significant differences were found between *MD:Touchscreen* and *VR:HMD* as well as *VR:LeapMotion* and *VR:Eye*. In all cases, *MD:Touchscreen* and *VR:HHC* were ranked favorably and there was no significant difference in their ease of error recovery.

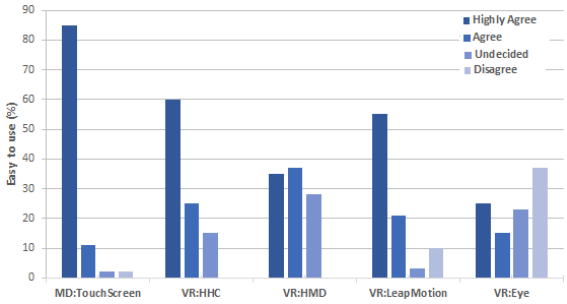


Figure 4.11: **Easy to use:** Participants survey on which technique was easier to use. Report shows that the mobile device touchscreen was easier to use.

4.6 Discussion

4.6.1 Login Speed

Our participants' performed significantly better on the mobile device but this was closely matched by their performance while using the *VR:HHC* and *VR:LeapMotion*. We believe that the familiarity of prior usage of mobile devices played a strong part in this outcome and surely with frequent usage of the VR interaction techniques their performances will improve. The data from the quantitative and qualitative (see Figure 4.10) analysis supports our observations.

4.6.2 Usability

Usability was determined by looking at the quantitative and qualitative data of this study. Our evaluation of the quantitative login speed, error rates and the participant‘s survey responses about error recovery, speed, likeability and ease of use indicates that the *VR:HHC* and *VR:LeapMotion* was considered as usable as the mobile device *MD:TouchScreen* used in this study (see Figure 4.12).

4.6.3 Shoulder-Surfing Resistance

The shoulder-surfing evaluation performed in section 4.5.1 indicates that PATTERN in VR has a very high resistance to shoulder-surfing (see Figure 4.9). Thus, making this solution highly secure for public usage where there might be multiple observers, we make this assertion with high confidence because of the fidelity of our experimental design and

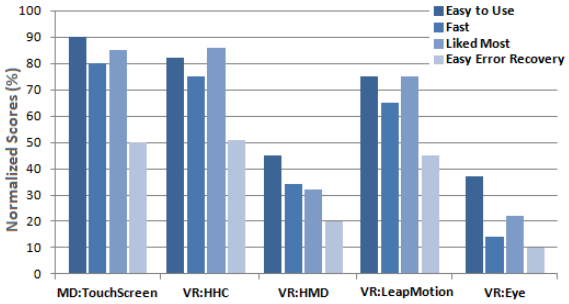


Figure 4.12: **LIKERT Survey:** Participants provided subjective feedback in a survey that was analyzed to generate the above information.

we are certain that field observations of participants can rarely be as accurate as our experiment.

4.7 Conclusion

We have presented a detailed and complete study to explore the outcome of porting the popular PATTERN authentication system into the virtual reality environment. This study shows that the PATTERN authentication system is well suited for VR. Participants performed equally similar within the mobile device and virtual reality environment. Participants performed better using VR interaction methods that were an extension of their hands, results indicate that the metrics of the *VR:HHC* and *VR:LeapMotion* are always similar to that of the mobile device. Virtual reality implementation of PATTERN is highly resistant to shoulder-surfing, thus a clear advantage when considering the fact that mobile device PATTERN has very little resistance to shoulder-surfing. We used the mobile device version of PATTERN as a control and the reports of the study as stated above, indicates that PATTERN in VR is moderately fast, functionally usable and highly resistant to shoulder-surfing, and this will open doors to the implementation of a familiar and robust PATTERN authentication systems into VR solutions.The novelty of this study was the numerous interaction methods we made available to the participants during the study via the virtual reality environment and teh fact that we were able to provide and enviroment that eliminated the risk of shoulder-surfing.

Chapter 5

BioMove : Exploration of Biometric identification from human Kinesiological activities in the Virtual Reality environment

5.1 Introduction

In the previous chapter, we reviewed the existing literature on Biometric authentication, hoping to answer research questions and identify the research gaps. In this chapter, we will explore Biometric authentication within the virtual reality environment with a special focus on transparent kinesiologically based authentication.

The use of virtual reality (VR) in a variety of applications has increased significantly in the last few years. The availability of inexpensive VR hardware together with rapid advances in their display and interaction peripherals have made VR popular. VR is currently being used in numerous domains such as medical-care [46], education [24], advertisement [37], shopping [117] and manufacturing [12]. High-end VR products are striving towards being fully wireless, reduced size, and improved personalization. These new features will open up a lot of usable possibilities and application domains. This new hardware also offers new possibilities to authenticate or identify users, other than traditional ways to login,

such as via PIN or other popular tethered methods. In this research, we provide the first *state-of-the-art* approach to identifying users from a natural kinesiological aspect in VR environments while including HMD integrated eye-tracking and gesture controllers. This achieved an accuracy of 97.2%, which is significantly higher than other approaches that authenticate users in real-world environments from sparse trajectories obtained using non-invasive or body-mounted sensors. There will be a strong demand for a robust, transparent, easy-to-use, and non-intrusive identification approach that allows these VR devices to be securely used by multiple users without any perceived or actual inconvenience. Because, as VR applications continue to grow, one aspect that has received little attention, to the best of our knowledge, is privacy and security issues of VR systems. User interaction in a VR environment is very different from other interactive systems, like mobile phones or computers. Various well understood security threats and attacks work in a completely different fashion within a VR environment, which makes well-known defense mechanisms ineffective or inapplicable. For example, directly implementing PIN or PATTERN authentication in VR environments, without any modifications, exposes the users to visual or observational attacks to a much larger extent than non-VR environments because of the relatively large movements of interactions in VR, and because most VR devices obscure the user's view, limiting their awareness of the external environment. These types of identification mechanisms will not only be impractical for VR systems but also does not leverage their unique and inherent features and hardware capabilities.

Our research focuses on the level of security needed to positively confirm the identity of a user using various known attributes that are distinct from other users engaged in a VR environment. In VR systems, users' body motion is captured to provide an immersive experience where their actions can be mimicked by avatar representations in real-time. This mimicry can range from the movements of their head, hand, leg, and other parts, including eyes, when a eye tracker is present in the VR device. VR systems present these movements that are as kinesiologically closed as possible to the users' movements [110, 74, 142]. Kinesiology is the study of the mechanics of body movements. A large body of literature exists on Kinesiology [73, 111, 55], and its results have been used by various disciplines including health, criminology, sports, rehabilitation and identification of people. Kinesiology defines and identifies co-joined movement behavioural patterns by the user's head and other limbs as an indication of specific movements in progress or about to start. For example, a user reaching to the ground to pick up an item must have the knees or back bent while the

head may face the particular direction according to the intended action. We argue that the kinesiological behavioural patterns exhibited by a user while interacting with a VR system to perform activities contain unique identifying cues that provide some measure of biometric confidence about the person using the VR environment. If these cues are reliably captured, using inertial and orientational sensors that now come in the VR devices, the user's movements can be recorded and used to create a biometric profile, which could then be used to provide an extra layer of security for the sensitive processes carried out in the VR space. It is possible to envision a transparent, easy-to-use, and non-intrusive identification method that may be used independently or as a second factor with a pre-existing VR identification system. We believe other studies, such as [151, 102], that are exploring the migration of standard mobile device identification systems such as PIN and PATTERN into virtual reality environments will benefit from an additional non-intrusive identification system.

In this thesis, we present BioMove, a behavioural pattern identification system that explores our above stated hypothesis. In particular, we investigate whether the head, limb, torso and eye movement patterns displayed by the user in the virtual reality space could be used as a biometric authenticating factor. To test the above hypothesis, we performed the following three activities.

1. **Kinesiologically designed VR environment.** We implemented a carefully designed VR environment to ensure the observation and recording of kinesiologically based movement patterns. We derived a set of typical tasks for an experiment that emphasize various movements of the head, eyes, arms, wrist, torso and legs [11] (see Figure 5.1).

2. **Focused tasks for data collection.** The participants are engaged in the task of placing the red balls into the cylindrical containers (see Figure 5.1) and the green/blue cubes into the rectangular enclosure. These task can be broken down primitively into elliptical movements on the XY-axis and rotational movements on the XZ-axis. We tracked and recorded various data from the head-mounted-display (HMD) VR device, an eye gaze tracker (GAZE) and the hand-held-controller (HHC) as the users interacted and moved items within the VR environment (see section 5.5.2 and 5.5.6).

Figure 5.1: **A screenshot of task based VR environment.** The environment was designed to elicit task based movements of users that allowed for biometric identification. Participants would perform movements that were primitively elliptical. In the above example, the user needed to relocate the ball from the bin to the container.

3. **VR Identity model.** The data derived from the task sessions was passed to a k-Nearest Neighbour (kNN) classifier to build an identity model, which was then used to identify the user during a future activity based on a preset threshold level of confidence (see Section 5.5.7).

5.2 Threat Model

In an attempt to improve the usability of sensitive VR applications or processes within them, we have identified three types of possible attackers. The *Type-I* attacker has no prior knowledge of the expected VR activities required and is mainly using a form of brute force attack. The *Type-II* attacker knows the required activity expected for identification (e.g. through watching a video clip or other observation methods), but has no other knowledge of

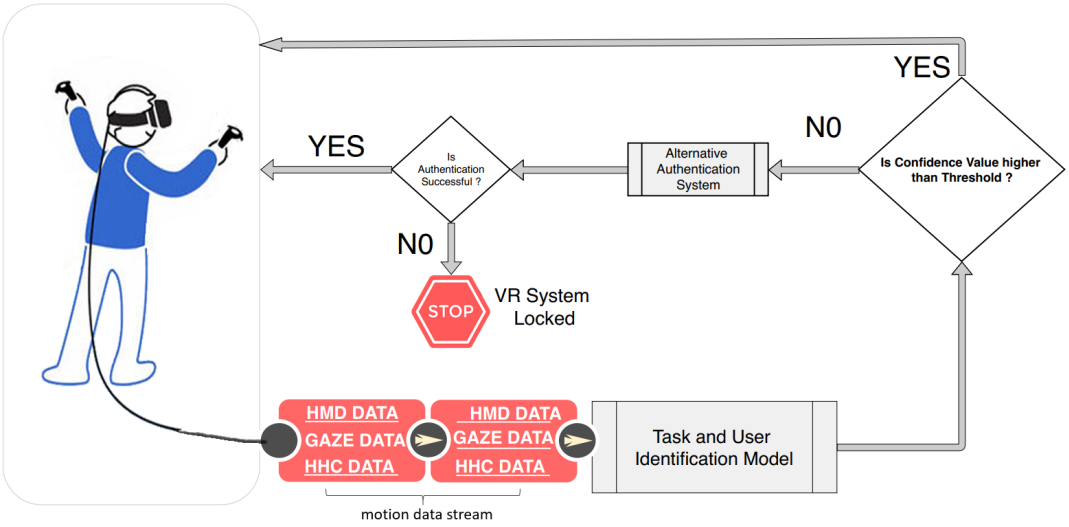


Figure 5.2: **A diagram of the BioMove biometric identification process.** As the user performs activities within the virtual reality environment, the *motion data stream* is passed to the *Identification Model* which determines the task and the user performing the task. A *confidence value* from the model is used to determine if the user is an authorized. If the user is not an authorized user, the VR session, for example, can be stopped.

the user's features that serve to identify them. The *Type-III* attacker is the most dangerous attacker because the identification activity is known and this attacker has similar physical features as the valid user. Our real-time continuous identification system negates the possibility of malicious or opportunistic attacks when the authorized user is temporarily absent or distracted, thereby denying an attacker access to the VR environment. In our threat model, the valid user of the VR system steps away, and the attacker (*Type-II* or *Type-III*) who has previously observed or has prior knowledge of the VR systems starts to use the system. After a series of uncharacteristic head and body movements while interacting with the VR environment, our method will lock the device or prompt the attacker to prove their identity via an alternative identification method. Figure 5.2 gives a highly abstracted view of how such an identification system might be designed. A numeric value known as *confidence value* determines if the activity belongs to a valid user. The confidence *threshold* value and the number and nature of uncharacteristic movements triggering the secondary identification mechanism would in practice be tuned to strike a balance between usability and security. In section 5.6, we performed a Whitebox penetration test using *Type-II* or *Type-III* attackers to determine the appropriate threshold confidence value. We make ref-

erence below to some examples of VR environments which might benefit from our methods.

Virtual Reality Gaming Applications. Numerous VR games are now becoming more multi-player oriented [109, 62]. A large number of these games require the user to perform different types of physically based interactions; as such, an identification method like BioMove would be very useful in these cases.

Virtual Reality based Shopping Applications. A growing number of online retailer and e-commerce platforms have started introducing virtual stores, allowing customers to transverse through virtual shops, pick and examine virtual 3D replicas of their product inventories [37, 12]. These companies, such as Alibaba and Amazon would benefit, from a transparent identification system that continuously verifies in the background its current user based on the motion patterns they exhibit during their shopping sessions.

5.3 Virtual reality task driven biometric identification

A study by Kupin *et al.* [62] was similar to our work, but in this study their 14 subjects picked up and threw balls at a target within the VR environment using the HTC VIVE hand-held controller. They achieved an accuracy of 92.86% using a simple distance metric, which is much lower than the 97.2% accuracy we achieve with our method. Another interestingly similar study by Pfeuffer *et al.* [109], which included HMD *integrated eye-tracking* and involved numerous activities such as *pointing, grabbing, walking, and typing* within the VR environment in an attempt to capture biometric discriminants for identification. This study was focused on the quality of the discrimnants, and reported accuracies of at best 63%.

5.4 Contribution of our work

The above study has some similarities to our work because they evaluated head or body movements within the VR space as a form of biometric discriminants. However, there are also significant differences that sets our work apart.

- **Biometric data sources**. Mustafa *et al.* [87], Li textitet al. [69], Sluganovic *et al.*, and Yi *et al.*. [149] solely relied on head movements to gather the unique significant

biometric features. This singular data input source increases the probability of malicious attacks. Our solution extracted biometric data from users' head, eyes, and hands in a kinesiologically conformative manner.

- **Applicable to VR environments that are based on active body movements**. Mustafa *et al.* [87] has pointed out that their solution focuses on a particular VR environment, whereas our solution can be used to authenticate in any VR environment where kinesiologically active movements exist or are used. Additionally, we track head and eye movements, which are basic actions exhibited while using a VR system.

- **Continuous vs one-time identification**. The solutions proposed by Li *et al.* [69] and Yi *et al.* [149] use a one-time identification model, allowing for a larger window of attack. Our study uses a continuous and dynamic identification model.

- **Identification domain**. The solutions in Li *et al.* [69] and Yi *et al.* [149] require the identification to occur in the physical domainvia smart glasses and wearable devices, whereas our solution uses the virtual domain, such as any applicable VR experience for identification, making our application more scalable and adaptable.

- **Multiple tasks**. The study by Kupin *et al.* [62] based their identification on a singular task of throwing the ball at a target, whereas our study involved 6 different VR tasks that includes a variety of kinesiological movements.

- **Penetration or vulnerability testing**. Mustafa *et al.* [87], Kupin *et al.* [62] and Pfeuffer *et al.* [109] did not provide penetration testing of their solution. We conducted a *Type-II* and *Type-III* whitebox penetration testing (see Section 5.9) and our results indicated high resistance to these attacks (see Figure 5.9).

5.5 Materials and Methods

5.5.1 Goals

In this study, our objective is to create a VR environment that allows users to perform a set of tasks. Our experiment comprises 6 different tasks, and each task is composed of a variable number of generic movements. We base these tasks on our review of the

literature on kinesiology and VR applications, thus they represent elliptical curves in three-dimensional space involving coordinated motions of the head, eyes, and hands. Using these tasks, we conducted a within-subjects study with 10 sessions per participant per day over a 2-day period. A session took an average of 2 minutes. Our experiment provided the data that we needed to investigate and understand whether biometric discriminants can be extracted from motion data recorded from multiple sensors. Another expectation we had was for our resultant system to be able to easily identify its users and specific tasks.

5.5.2 Experimental Design

The participant movements are grouped into a set of tasks, which represent the *raw data* of our study, which will help derive the *features* required in our analysis. The components of the movement and the resultant tasks are explained below.

User Tasks

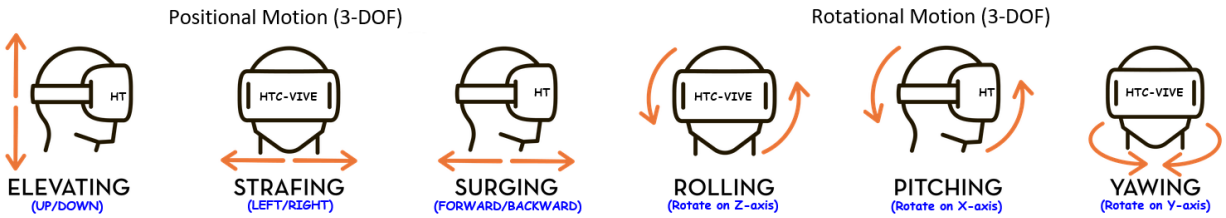
The movements were encapsulated into a task. We designed two variants of this task, one dealt with *balls* and the other with *cubes*. The participants were given the task of grabbing, transporting and dropping balls and cubes into containers strategically placed within the VR environment (see Figure 5.1). This ensures that kinesiologically valid motion data would be captured during our experiments. We would then pass the collected data into a kNN classifier and train an identification model with a high confidence value output. Below are the variables we are tracking:

The raw data sources

- **Task 1:** Interacting with Balls in VR environment.
- **Task 2:** Interacting with Cubes in VR environment.
- **Participant static metrics such as** height, arm length, and waist height.

The features tracked

- Head-Mounted Display positional, rotational data.
- Eye tracking gaze positional data.



(a) (b)

Figure 5.3: **Possible 6-DOF VR Movements.** (a) [**Positional**] **Motion** is the location of the object in the 3D world space. There are 3 possible positions motions (3-DOF). **(i)** ***Elevation:*** is where the head/hand moves up or down *(i.e. when bending down or standing up)* **(ii)** ***Strafe:*** is where the head/hand moves left or right *(i.e. sidestepping)*. (iii) ***Surge:*** is where the head/hand moves forwards or backwards *(i.e. when walking)*. **(b)** [**Rotational Motion**] is the orientation of the object in 3D world space. There are 3 possible orients (3-DOF). **(i)** ***Roll:*** is where the head/hand pivots side to side *(i.e. peeking around a corner)*. **(ii)** ***Pitch:*** is where the head/hand tilts along a vertical axis *(i.e. when looking up or down)*. **(iii)** ***Yaw:*** is where the head/hand swivels along a horizontal axis *(i.e. looking left or right)*.

- Hand-Held Controller positional and rotational data.

Movements

Each movement involves three main aspects of the body to varying degrees. These aspects are:

- ***Head Movements***. The head moves through the six degree of freedom (6-DOF) while the participant targets, rotates and translates within the VR environment (see Figure 5.3). This is captured via the sensors in the HMD.

- ***Eye Movements***. The eyes move as the participant locates, targets, grabs and moves the objects within the VR environment. This is captured using an eye tracking system embedded in the HMD (Figure 4.3b).

- ***Hand Movements***. The hand moves through the 6-DOF while the participant grabs, transports, rotates, targets and drops the objects of interest (see Figure 5.3). This is captured via the head-held controller (HHC) (see Figure 4.3a).

5.5.3 Research Ethics

All subjects gave their informed consent for inclusion before they participated in the study. The study was conducted in accordance with the Declaration of Helsinki. The protocol was reviewed by the XJTLU Research Ethics Committee and found to be low risk research.

5.5.4 Apparatus

The Virtual Reality Environment

We created a VR environment, with Unity3D and C# on a Windows 10 PC *(Intel Core i7-6700, 128GB RAM, NVIDIA GeForce 1080)* to assist in the collection of our experimental data. In our VR environment, positioned in front of the participant is a wooden stand with three horizontal poles that are vertically spaced dynamically to be reachable based on the participant's height (see Figure 5.4). Furthermore, at the opposite end of each horizontal pole is a cylindrical container and a cubic container that will be the final destination of the objects that the participants interact with during the session. Lastly, on the left side of the participant is a stack of cubes and to the right side of the user is a stack of balls. The VR environment mimics the real-world and objects follow the laws of physics and their composite materials. The participant is allowed to move around within the environment.

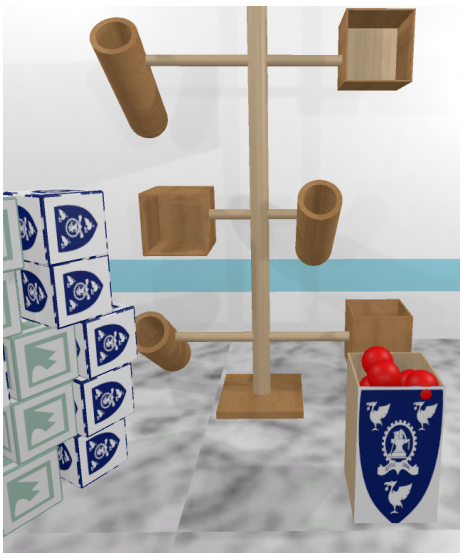


Figure 5.4: **VR environment layout:** The environment consist of a wooden stand, balls and cubes that participant relocate into the respective containers.

The Interaction Devices

The feeling of immersivness of VR is due to the ability to interact realistically with objects within the environment. For this experiment we used the HTC Vive VR system. Our participants would interact using the following:

- **Head**. The VR headset containing the HMD has inertial motion sensors to estimate the participant's head position and rotation. These sensors can capture data concerning the HMD and constantly update the VR environment according to head movements. The HMD allows us to extract the positional coordinate and rotational, acceleration and velocity data for our experiment (see Figure 5.3).
- **Eyes**. The eye-tracking hardware, called aGlass [3], was installed inside the HMD to track the participants' gaze as they performed the tasks. It can track the the positional coordinates (x,y) or direction where the participant is looking at within the virtual scene. The eye tracker was calibrated with a 9-point accuracy method.
- **Hands**. The hand-held controller (HHC) allows participants to replicate their hand motion and usage within the VR scene to grab, move and release VR objects. The HHC also provides the positional coordinates, rotational, acceleration and velocity data during the experiment.

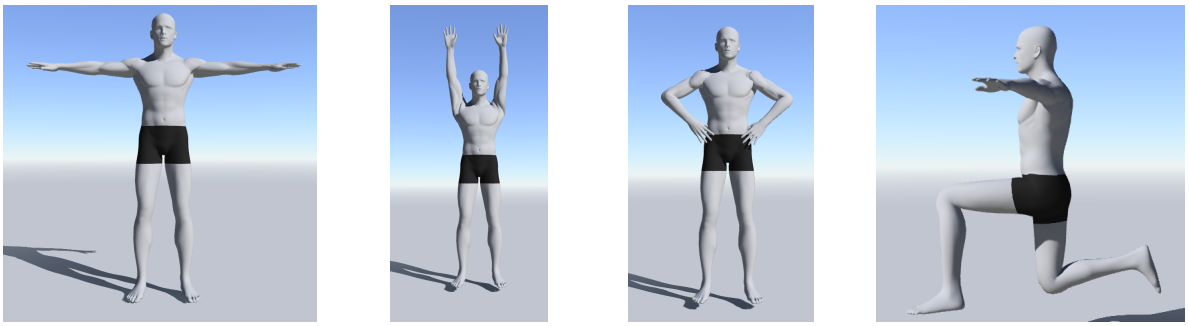
5.5.5 Participants

We enlisted 25 participants from a local university. Our pre-testing survey reveals that 72% of the participants were between the ages of 18 to 29 and only 3 participants were left-handed. All were aware of VR technologies, but only 64% of them had previously used a VR application. All participated voluntarily without any financial remuneration.

5.5.6 Task and Procedures

Each session started with a brief introduction to the experiment. Then the participants were shown a 2 minute tutorial video that demonstrated the intended activity and how the VR devices were used, after which they were allowed to practice each task a couple of times. The physical measurement to capture the user height, arm span, waistline and knee height was done using the hand-held controllers as a measuring tool (see Figure 5.5). These measurements were used to configure the VR environment to ensure that all

participants have similar experiences within the VR environment. For example, the VR objects are adjusted to the participants physical attributes so all items can be reachable. Additionally, eye tracking 9-point calibration was done once and the configuration data was stored with the participant ID for future use. A session took approximately 2 minutes, during which the participants would grab, relocate, drop 3 balls and 3 cubes into their respective containers (See Figure 5.1). Each participant was allowed to rest for 2 minutes after the completion of 5 out of 10 sessions.



(a) User Arm Span (b) User Reach (c) User Waist height (d) User Knee height

Figure 5.5: **Pre-Experiment measurements**: The Participants' body metrics were taken before the initial experiment session commenced. The data was used to configure the VR environment to ensure that all participants would have similar experiences in the environment.

5.5.7 Data and Feature Processing

We collected 5 features from the raw data consistently as the participants performed the tasks in the VR environment. We logged the data at the rate of *25 readings per second* (25Hz), combining the data stream from the HHC, HMD, and eye tracker to create a *movement data vector* with supporting metadata. This component movement data vector or ***movement vector*** is shown below:

- **HHC and HMD:**
  - Positional Data: x, y, z.
  - Rotational Data: x, y, z, w. *(Quaternion format)*
- **Eye Tracking Device:**

  - Positional Data: x, y.

- **Miscellaneous Metadata:**
  - Task performed: t, (where $1 \leq t \leq 6$). *(We have 6 different tasks that are performed in a Session)*
  - Time Stamp : yyyy-mm-dd-hh-M-ss-zzz.

Motion Data ReSampling

In the experiment, each participant performed numerous sessions in the VR environment and their session completion interval varied. Consequently, we needed to *resample* the data to create a consistent set of data for all participants. Each participant performed the task at different speeds while each task was defined by a sequence of movement vectors which were captured at *25 movement vectors* per second (25Hz). For example, if participant A and B completed *Task 1* in 50 seconds and 100 seconds respectively, participant B would have 2500 movement vector readings, while participant A has 1250 readings for the same identical task. Our resample process allowed us to select 1250 movement vector readings from participant B's data, ensuring that all participants would have the same number of movement vector readings. Below are some definitions:

- **Session:** A Session **S** is a set of task **t** (see Equation 5.1).

$$S = \{t_1, ..., t_6\} \ \ where\ cardinality\ |S| = 6 \tag{5.1}$$

- **Task:** A Task **T** is a set of movement vectors **m** (see Equation 5.2).

$$T = \{m_1, ..., m_n\} \ \ where\ cardinality\ |T| = n \tag{5.2}$$

- **Median:** The median $\boldsymbol{D}$ of the cardinality of movement vectors $|T|$ for each type of tasks $\{t_1, ..., t_6\}$ across all sessions **S** in the experiment are determined as follows :

For Each Task type T_x (where $1 \leq x \leq 6$) in the Experiment

$$D_x = Median(|T_x|_1, ..., |T_x|_n) \tag{5.3}$$

where $|T_x|$ is the cardinality of a set of movements of task type x

- **Resampling Process:** The Median or sample size D_x has been determined for each Task type T_x (see Equation 5.3). The Task movement count $|T|$ is *resampled* to the relevant D_x movement count. Therefore, at the end of the resampling process each task group would have the same number of movements vectors, *which in this case is the median value* ***D****,* across all participants, and any task that does not meet the above resampling process criteria is discarded as outliers. The resampling process resulted in 65,241 valid movement vectors (see Section 5.5.7 and Algorithm 1).

As stated earlier, we collected data from 25 participants initially. We later had to remove the data of 4 participants due to invalid eye-tracking data, cause by a hardware issue, we also removed the data of 3 and 4 other participants due to inconsistent data from the HHC and HMD devices respectively. The remaining 14 participants' data was resampled according to the steps in Section 5.5.7 . This process ***left us with 10 participants*** whose 6 task sessions met the resampling requirements.

5.5.8 Machine Learning Classification Framework

The experiment produced a total of 65,241 movement vectors after the resampling process and removal of outliers. We divided the data into 80% for *training* and the remaining 20% was reserved as *testing*. The classification was performed using the MatLab platform, and to gain insights into how different classifications methods might affect performance we employed the built-in *MatLab Classification Learner App*, which automatically performed supervised machine learning tasks such as interactively exploring data, selecting features, training models and assessing results. Models tested included decision trees, discriminant analysis, support vector machines, logistic regression, k-nearest neighbors (kNN), naive Bayes, and ensemble classification. We also enabled the PCA (principal component analysis) feature to reduce the data dimensionality using PCA on the predictor data and then transform the data before training the models. We selected the k-Nearest Neighbour (kNN) classifier because KNN is a non-parametric, lazy learning algorithm and best suited for our movement vector datasets in which the data points are separated into several classes to predict the classification of a new sample point. KNN is also very sensitive to outliers and bad features. We strongly believe the high-level of accuracy observed is due to our resampling process (see Section 5.5.7). Additionally, KNN is less computationally intensive and will work optimally on all types of low powered mobile devices.

Algorithm 1: Movement vector Resample algorithm

Input : Arrays of **Task** objects and precalulated Median of movement vectors for each Task type

Output: Array of Task objects with movement vectors resampled to match corresponding task type median

```
1  Function ReSampleTask(TaskObj[ ] t, TaskTypeMedian[ ] d)
2      TaskObj[ ] DownSampleTaskObj = [ ];
3      for taskType ← 1 to 6 do
4          // get all the Task objects of a TaskType.
5          TaskObj[ ] tmpT = t.getSubset(taskType);
6          // get the movement vector Median value for that TaskType.
7          medianValue = d[taskType];
8          foreach task in tmpT do
9              taskMovementCount = task.movement.count();
10             if taskMovementCount >= medianValue then
11                 // round down the value.
12                 stepvalue = round(taskMovementCount/medianValue);
13                 movementPos = 0;
14                 MovementVector tmpMovement;
15                 // ReSample the movement vectors
16                 while movementPos < taskMovementCount do
17                     tmpMovement.add(task.movement[movementPos]);
18                     movementPos = movementPos + stepvalue;
19                 end while
20                 // copy the resampled movemeent vector back into the task
                      object
21                 task.movement = tmpMovement;
22                 DownSampleTaskObj.add(task);
23             end if
24         end foreach
25     end for
26     return DownSampleTaskObj;
27 end
```

Finally, after cross-validating each model type, the MatLab Data Browser displayed each model and its k-fold, cross-validated classification accuracy, and highlighted the kNN model as having the best accuracy of 97.2% among other classifiers. The goal of cross-validation is to test the model's ability to predict new data that was not used in estimating it. With this goal in mind, one wants to estimate how accurately a predictive model will perform in practice, therefore a model is given a dataset of known data on which training is run (training dataset), and a dataset of unknown data against which the model is tested. The output is the predictive accuracy of the model.

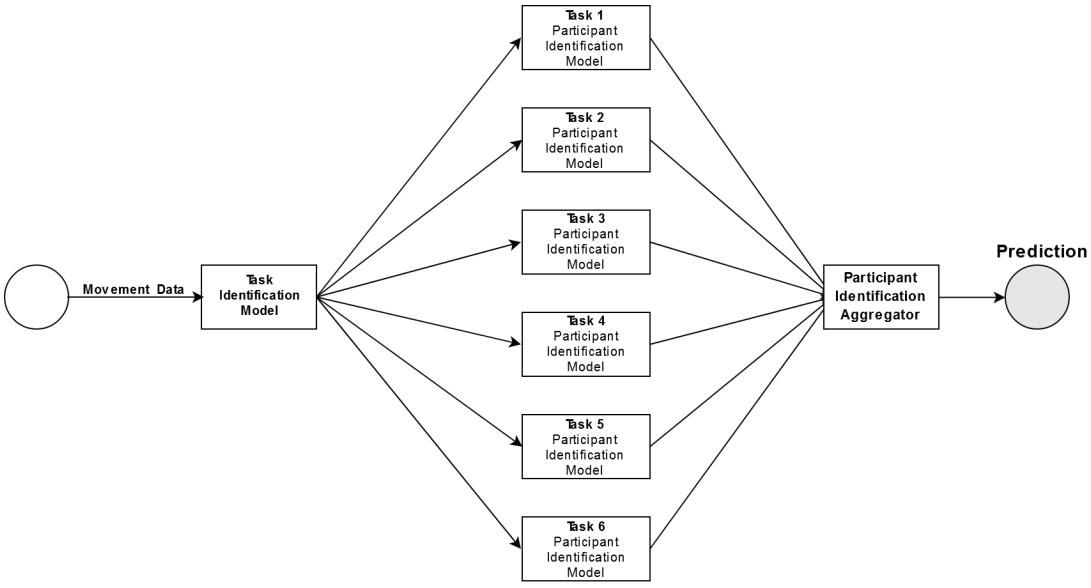


Figure 5.6: **Participant Identification Process flow:** As the participant performs the task or motion within the VR environment, the actions are broken into identifiable task by the *Task Identification model*. The output is then sent to the appropriate task focused *participant identification model*. The output of the identification process is then fed into an *aggregator* that attaches a confidence value and predictively confirms the valid participant

Identification

For our identification scenario, we had to train on two different sets of predictors that resulted in models with different identification functions. We obtained two training models. The *first model* (the Task Identification model) focused on identifying the type of tasks $(t_1, ..., t_6)$ performed and the *second model* (the Participant Identification model) focused

on determining the participants $(P_1, ..., P_n)$ performing the tasks (see Figure 5.6). As the participants performed the task or motions within the VR environment, their physical actions or movements were broken or sampled into identifiable tasks by the *task identification model*. The output was then sent to the appropriate task focused *participant identification model*. The output of the identification process was then fed into an *aggregator* that would attach an accuracy value and predictively confirm the identity of each participant.

- **Task Identification Model**. This model is trained on identifying the task performed by the participants based of the movement vector streams. The resulting model makes a prediction of the task t_i from the set of all possible tasks T. This stage allows a practical implementation where the results of this stage are used to select the correct participant identification model, thereby increasing accuracy and response time.

- **Participant Identification Model**. This model is trained to identify participants performing a particular task. The resulting model makes a prediction of the participant p_i from the set of all participants P. In this scenario we have $n = 6$ tasks thus resulting in 6 different participant identification models. We argue that task specific model results in higher accuracy and faster identification systems (see Figure 5.6).

- **Participant Identification Aggregator**. The Aggregator module receives the output of the participant identification model and uses the data to produce a weighted average and frequency analysis across the tasks. The output of this aggregator module is the participant ID and the prediction accuracy score of the participant with the highest prediction value across the 6 tasks (see Figure 5.6).

5.6 Whitebox Penetration Testing

Penetration testing evaluates the security of a system against malicious attacks to identify vulnerabilities, and this requires us to use Whitebox techniques. During the study, three high resolution video cameras were placed at the TOP, LEFT and FRONT locations of the participant to record the external physical actions of our participants (see Figure 5.7). We selected the participant P6 because this participant had the *highest* prediction accuracy of 100% and participant P3 with the *lowest* prediction accuracy of 85% (see Figure 5.8).

(a) (b)

Figure 5.7: **Task Sessions: (a)** Participant performing a task while being recorded by 3 cameras placed at *TOP, LEFT, FRONT* locations. As shown in the picture the actions performed by the participant are monitored and recorded (see TV screen) with emphasis placed on the head and hand movements. This recording is later viewed by an attacker in an attempt to emulate the participant's movement. **(b)** A participant stretches to maximum height as she performs the task. These kinesiological movements are captured and processed for unique biometric discriminants

Two groups of 6 attackers *(3 females, 3 males)* were selected. The first group consist of users who were similar in *height*, *arm span* and *weight (CloneMale **CM** or CloneFemale **CF**)* to the valid participant. The second group consist of randomly selected users *(RandomMale **RM** or RandomFemale **RF**)*. Each attacker performed 5 sessions each of *Task 1* to *Task 6* after watching videos of two the valid participants (P3, P6) performing these tasks. We passed the captured attacker movement task data into the kNN model trained for P3 and P6 and tracked the results based on the level of confidence values (see Figure 5.9). As shown in Figure 5.9, the attackers did not attain the minimum confidence value required to qualify as a valid user. We also observed that the attackers with similar physical features as the valid users had higher confidence levels, these levels are even higher

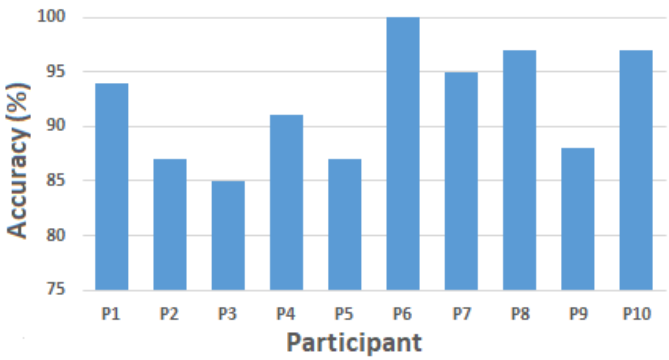


Figure 5.8: **Accuracy per participant across all tasks:** The prediction accuracy of participants movements across all tasks.

when attackers and valid users are of a similar gender.

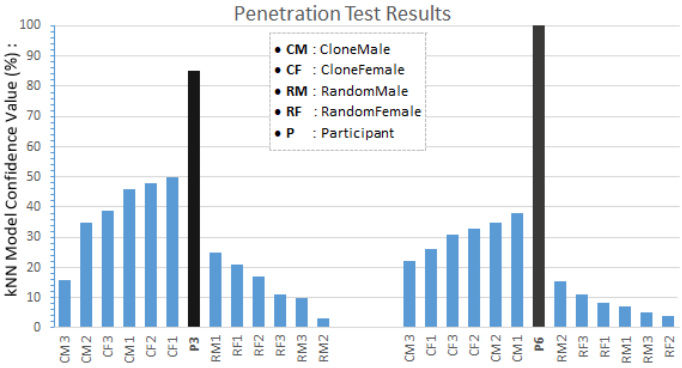


Figure 5.9: **WhiteBox Penetration Test:** Attackers mimicking the tasks performed by the valid participants P3 and P6 in an attempt to breach the security of the BioMove identification system. Results indicate different level of confidence values shown above. Attackers with similar physical features to the valid users have higher confidence values.

5.7 Results and Discussion

We achieved highly accurate results in identifying participants within the VR environment. The identification process involves first identifying the task and then identifying the participant. On the Windows 10 PC *(Intel Core i7-6700, 128GB RAM, NVIDIA GeForce 1080)*, we clocked the GPU down to 1600 MHz and observed an average identification processing speed of

35 milliseconds per 1000 identification evaluations. At this speed, the response is instantaneous from the users perspective. Overall, we achieved a cross-validated classification accuracy of 97.2% and an error rate of less than 3% using the testing data and additional study data on the trained identification model. We generated a confusion matrix that summarizes the actual performance of the kNN algorithm, thus providing us with a view into what the model handled correctly and what types of errors it was making (see Figure 5.10). Furthermore, results from the movement data identification of all participants across all tasks is shown in Figure 5.8. Our whitebox penetration test indicates that attackers impersonating the valid participants resulted in less than 50% accuracy value, thus a accuracy value threshold above 80% will be sufficient to protect against malicious attacks producing false positive identifications. The penetration test also confirms that attackers who are physically similar to the valid participant produce higher accuracy values (see Figure 5.9).

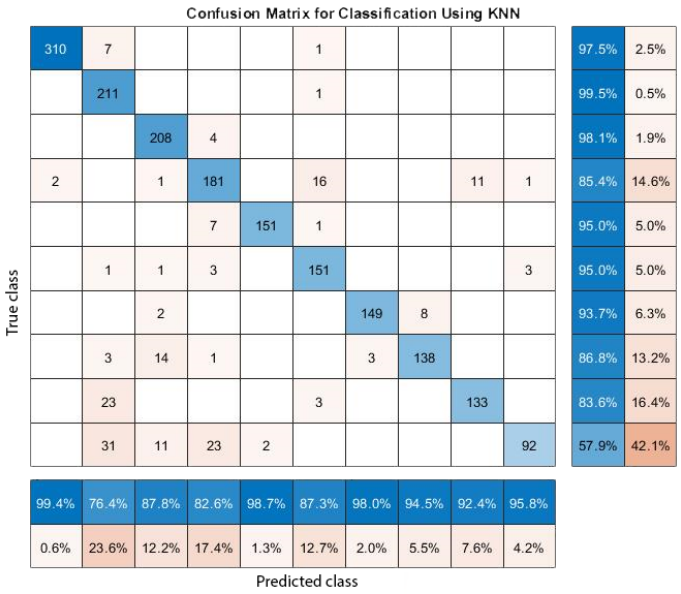


Figure 5.10: **kNN Classifier Confusion Matrix:** A confusion matrix summarizes the performance of a classification algorithm.It gives a better idea of what your classification model is getting right and what types of errors it is making. Classification accuracy alone can be misleading because we have more than two classes in our dataset.

The potential application of this research is a form of universal identification module that is hosted by the VR device firmware system and independent of any specific VR soft-

ware application, be it a game or productivity tool. This solution may be implemented using the low-level Open Broadcaster Software (OBS) OpenVR [104] application programming interface (API) kit or the new OSVR [106] input plugin that mirrors all movement data at the hardware level and dynamically hooks into base GUI modules of all high-level VR applications to interrupt their session if the transparent non-intrusive identification (TNI) based on these movement data fails (see Figure 5.2). This proposed universal identification module can also be configured to trigger the local identification process on the high-level VR session it interrupted as a means of providing a second-factor identification and allowing the system to request the user to provide an alternative identification. Our research was aimed at users between the ages of 18 to 30, which is the largest demography of user groups of VR systems [77]. Although, looking at the aging process and how that affects the use of the VR identification system is interesting and important to explore, so that we can have more targeted systems for each specific group; it is outside of the scope of the thesis, and therefore a part of our future work.

5.8 Conclusion

Our study provides a preview into what can be achievable in terms of using kinesiological movements within virtual Reality (VR) environments for biometric identification. The novelty of this study emanates from our process of using machine learning and task derived kinesiology in the virtual reality environment to biometrically identify the users. We evaluated 65,241 dataset of head, eyes and hand movements using machine learning to create a continuous biometric identification system. In our best configuration, we attained a classification accuracy of 97.2%. These results indicate that the head and body movement based biometric identification holds promise that points to the possibility for continuously identifying and authenticating participants in VR systems. In practice our method would not have to be VR application specific since we have distilled the primitive body movement patterns that are similar across different VR environments. For example, a movement biometric template captured in the core VR systems can be used to authenticate in a VR gaming application or banking application. We also determined that attacks on our BioMove identification system would require a highly sophisticated attacker. We argue that simultaneously providing the system false-positive data vectors such as eye, head and hand movement vectors that are kinesiologically replicating a valid participant is extremely difficult. In the future, we plan to extend our research to different groups

and evaluate the relative accuracy and robustness of our approach across multiple groups, especially taking into account the effect of aging on the kinesiological movements of users. In addition, future work will explore integrating our solution into pre-existing VR environment frameworks when VR hardware manufacturers provide APIs that allow us to embed our systems into their firmware. As a result, we will have a real-time application that will be totally responsive and transparent to users while interacting with a VR device doing typical tasks such playing a game, doing learning activities, and exploring multi-user worlds. We believe that our research can serve as a second-factor authentication system where the verification will be 1-to-1.

Chapter 6

Conclusion

In this thesis, we introduce Usable Secure Interfaces for Mobile Devices, and our main objective was to examine the attributes of our established hypotheses. We achieved this through the evaluation of existing literature, extensive prototype developments, and empirical experiments. The results and knowledge from previous experiments were used as a foundation for further evaluation as we evolved our research through various user environments such as from mobile phone devices into virtual reality devices while ensuring that the evaluated systems remain the same or similarly represented in the new environment to maintain consistency of operations and ecological viability to our participants.

Our research produced two novel solutions and a novel virtual reality evaluation of pre-existing authentications systems. Firstly, the SemanticLock graphical authentication system, as explained in Chapter 3, defined a state-of-the-art method of usable security for mobile devices using memory enchanced semantic methods for password creation. Secondly, the porting of the popular PATTERN authentication system, as explained in Chapter 4, into the virtual reality environment to allow a multitude of interaction methods to be tested on the authentication system. Thirdly, the BioMove authentication system, as explained in Chapter 5, used the unique aspect of human kinesiology and machine learning to positively predict the identity of users performing task within the virtual reality environment.

6.1 Contributions

Specifically, our contributions to the research questions of this thesis are listed in details as follows:

1. **Re-conceptualizing mobile device interfaces to make them both secure and usable:** We designed and developed SemanticLock to explore a graphical authentication system that was as usable as other conventional methods while offering better memorability and security. These features were achieved by combining a semantically meaningful story-based password to improve memorability with a carefully designed password space to improve user-selected password entropy. Our memorability study showed that users retained SemanticLock passwords much more easily than PIN or PATTERN, even after two weeks of non-use. In the final analysis, our participants both quantitatively and qualitatively found SemanticLock more usable and secure than current mainstream authentication methods.

2. **The acceptable levels of complexity an interface could have to be secure and yet still usable:** We developed and presented a detailed and complete study to explore the outcome of porting the popular PATTERN authentication system into the virtual reality environment. Using observations from existing literature, we carefully recreated the virtual reality (VR) version of PATTERN to function as closely as possible to the mobile device version. Our study used the mobile device version of PATTERN as a control and the reports of the study indicate that PATTERN in VR is moderately fast, functionally usable and highly resistant to shoulder-surfing, and this will ease the implementation of a familiar and robust PATTERN authentication systems into VR solutions.

3. **The technological impediments that make it diffcult to develop secure interfaces:** Our study provides a glimpse into what can be achievable in terms of using kinesiological movements within the VR environment for biometric authentication. We evaluated datasets of head, eyes and hand movements and used machine learning processes that resulted in models with high classification accuracy allowing for a continuous biometric authentication system. Our results indicate that the head and body movement-based biometric authentication holds the promise that points to the possibility of continuously identifying and authenticating participants in VR systems.

it is noteworthy that in practice our method would not have to be VR application-specific since we have distilled the primitive body movement patterns that are similar across different VR environments. We also determined that attacks on our BioMove authentication system would require a highly sophisticated attacker. We are able to obtain a trained model classification or identification accuracy of 97.2%.

6.2 Future Work

In this thesis, we have presented works that demonstrate novel tremendous practical potential in real-world applications of mobile security. In this section, we describe several specific future projects that could be achieved.

6.2.1 SemanticLock Authentication

Building on the results of our 3 weeks study, we hope to implement a larger public based study that will involve millions of users across the world in a real-world environment. The SemanticLock will be rewritten as an integrated replacement Login service and made available on all mobile device platforms then released for download. Other improvements suchs as user defined icons will be possible. The usage data received from these public participants will provide better insights and spotlight areas for further improvement. We hope in the long run the SemanticLock will be a popular viable alternative for authentication on mobile devices in the public software domain.

6.2.2 PATTERN Authentication in VR

Although our study outcomes were satisfactory, we recognize that there is room for improvement due to the short periods of this study. We strongly believe that participants were unable to adequately get familiar with many of the VR interaction techniques that were not inherently intuitive. The above observation might have had some impact on the study outcomes, and we believe there is an opportunity for a future study that fully engages the participants in long periods of VR sessions that requires a series of authentication stages as the session progresses. It is our projection that great improvement will be seen in the participant's login speed, usability, and error-recovery. Lastly, results from the VR shoulder-surfing indicates that the VR implementation of PATTERN has a high resistance,

we believe as a future study, it will be interesting to use machine-learning techniques in predicting the participants passwords from the recorded videos of their login activities.

6.2.3 BioMove Authentication

One limitation of this research is the unvailability of a large dataset with the data that is needed to explore and obtain accurate FAR, FRR and EER values to achieve authentication. We plan to continue this research and collect data from a much larger population and explore ways to provide authentication methods for VR systems. Secondly, because our research was primarily focused on one of the most common user groups (i.e., those between the ages of 18-30), we only recruited participants in this category. In the future, we plan to extend our research to different age and gender groups and evaluate the relative accuracy and robustness of our approach across multiple groups, especially taking into account the effect of aging on the kinesiological movements of users. In addition, future work will explore integrating our solution into pre-existing VR environment frameworks when VR hardware manufacturers provide APIs that allow us to embed our systems into their firmware. As a result, we will have a real-time application that will be totally responsive and transparent to users while interacting with a VR device doing typical tasks such playing a game, doing learning activities, and exploring multi-user worlds. We believe that our research can serve as a second-factor authentication system where the verification will be 1-to-1. In short, a larger and more diverse group of participants is required to enable us to determine accurate values of FAR, FRR and EER, a more focused look at the effects of aging on VR Identifications systems, and deployment of the BioMove systems into totally untethered VR hardware will provide the data and insights that we require to design and develop a more comprehensive solution to allow accurate and robust identification and authentication of users in VR systems.

Bibliography

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 3751–3763, New York, NY, USA, 2017. ACM.

[2] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. In *2008 Second Asia International Conference on Modelling Simulation (AMS)*, pages 396–403, May 2008.

[3] aGlass Eyetracking (7invensun) Upgrade kit. Htc vive hmd- aglass eyetracking kit, 2018. [Online; accessed April 4, 2019].

[4] F. A. Alsulaiman and A. E. Saddik. A novel 3d graphical password schema. In *2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems*, pages 125–128, July 2006.

[5] Yomna Aly, Cosmin Munteanu, Stefania Raimondo, Alan Yusheng Wu, and Molly Wei. Spin-lock gesture authentication for mobile devices. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, MobileHCI '16, pages 775–782, New York, NY, USA, 2016. ACM.

[6] Bander A. Alzahrani, Martin J. Reed, and Vassilios G. Vassilakis. Resistance against brute-force attacks on stateless forwarding in information centric networking. In *Proceedings of the Eleventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ANCS '15, pages 193–194, Washington, DC, USA, 2015. IEEE Computer Society.

[7] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '13, pages 1–6, New York, NY, USA, 2013. ACM.

[8] Apple TouchID. Apple touchid, fingerprint scanner, 2013. [Online; accessed February 20, 2018].

[9] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. Is bigger better? comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In *Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015, pages 301–310, New York, NY, USA, 2015. ACM.

[10] Marios Belk, Andreas Pamboris, Christos Fidas, Christina Katsini, Nikolaos Avouris, and George Samaras. Sweet-spotting security and usability for intelligent graphical authentication mechanisms. In *Proceedings of the International Conference on Web Intelligence*, WI '17, pages 252–259, New York, NY, USA, 2017. ACM.

[11] Chiraz BenAbdelkader, Ross Cutler, and Larry Davis. View-invariant estimation of height and stride for gait recognition. In *International Workshop on Biometric Authentication*, pages 155–167. Springer, 2002.

[12] Leif P Berg and Judy M Vance. Industry use of virtual reality in product design and manufacturing: a survey. *Virtual reality*, 21(1):1–17, 2017.

[13] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, September 2012.

[14] G. Blonder. Graphical password. *In Lucent Technologies, Inc*, 1996.

[15] J. Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy*, pages 538–552, May 2012.

[16] Joseph Bonneau. Statistical metrics for individual password strength. In *Proceedings of the 20th International Conference on Security Protocols*, SP'12, pages 76–86, Berlin, Heidelberg, 2012. Springer-Verlag.

[17] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A birthday present every eleven wallets? the security of customer-chosen banking pins. In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security*, pages 25–40, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[18] P. Bours and A. Evensen. The shakespeare experiment: Preliminary results for the recognition of a person based on the sound of walking. In *2017 International Carnahan Conference on Security Technology (ICCST)*, pages 1–6, Oct 2017.

[19] Sacha Brostoff and M. Angela Sasse. Are passfaces more usable than passwords? a field trial investigation. In Sharon McDonald, Yvonne Waern, and Gilbert Cockton, editors, *People and Computers XIV — Usability or Else!*, pages 405–424, London, 2000. Springer London.

[20] Andreas Bulling, Florian Alt, and Albrecht Schmidt. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 3011–3020, New York, NY, USA, 2012. ACM.

[21] Daniel Buschek, Fabian Hartmann, Emanuel von Zezschwitz, Alexander De Luca, and Florian Alt. SnapApp: Reducing Authentication Overhead with a Time-Constrained Fast Unlock Option. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 3736–3747, New York, NY, USA, 2016. ACM.

[22] Ashley A. Cain, Steffen Werner, and Jeremiah D. Still. Graphical authentication resistance to over-the-shoulder-attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '17, pages 2416–2422, New York, NY, USA, 2017. ACM.

[23] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. Boosting the guessing attack performance on android lock patterns with smudge attacks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, pages 313–326, New York, NY, USA, 2017. ACM.

[24] Magesh Chandramouli and Justin Heffron. A desktop vr-based hci framework for programming instruction. In *2015 IEEE Integrated STEM Education Conference*, pages 129–134. IEEE, 2015.

[25] Hsin-Yi Chiang and Sonia Chiasson. Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 251–260, New York, NY, USA, 2013. ACM.

[26] Sonia Chiasson, Robert Biddle, and P. C. van Oorschot. A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 1–12, New York, NY, USA, 2007. ACM.

[27] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. *Int. J. Inf. Secur.*, 8(6):387–398, October 2009.

[28] Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. Graphical password authentication using cued click points. In *Proceedings of the 12th European Conference on Research in Computer Security*, ESORICS'07, pages 359–374, Berlin, Heidelberg, 2007. Springer-Verlag.

[29] P. Corcoran and C. Costache. Biometric technology and smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts. *IEEE Consumer Electronics Magazine*, 5(2):70–78, April 2016.

[30] Darren Davis, Fabian Monrose, and Michael K. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, pages 11–11, Berkeley, CA, USA, 2004. USENIX Association.

[31] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. Colorpin: Securing pin entry through indirect input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1103–1106, New York, NY, USA, 2010. ACM.

[32] L. de Wilde, L. Spreeuwers, and R. Veldhuis. Exploring how user routine affects the recognition performance of a lock pattern. In *2015 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8, Sept 2015.

[33] Rachna Dhamija and Adrian Perrig. Déjà vu: A user study using images for authentication. In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9*, SSYM'00, pages 4–4, Berkeley, CA, USA, 2000. USENIX Association.

[34] Paul Dunphy, Andreas P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 3:1–3:12, New York, NY, USA, 2010. ACM.

[35] Paul Dunphy, James Nicholson, and Patrick Olivier. Securing passfaces for description. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, pages 24–35, New York, NY, USA, 2008. ACM.

[36] Simon Eberz, K Rasmussen, Vincent Lenders, and Ivan Martinovic. Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics. 2015.

[37] Hui Fang, Jie Zhang, Murat Şensoy, and Nadia Magnenat-Thalmann. Reputation mechanism for e-commerce in virtual reality environments. *Electronic Commerce Research and Applications*, 13(6):409–422, 2014.

[38] A. L. Fantana, S. Ramachandran, C. H. Schunck, and M. Talamo. Movement based biometric authentication with smartphones. In *2015 International Carnahan Conference on Security Technology (ICCST)*, pages 235–239, Sept 2015.

[39] S. M. H. S. S. Fathima and A. Valanarasi. Human gait recognition using relevance vector machine classifier. In *2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, pages 564–568, May 2016.

[40] T. Feng, X. Zhao, and W. Shi. Investigating mobile device picking-up motion as a novel biometric modality. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–6, Sept 2013.

[41] FOVE Eye. Fove eye tracking hmd, 2018. [Online; accessed May 4, 2018].

[42] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1):136–148, 2013.

[43] Fujitsu Mover F505i. Fujitsu mover f505i, first in japan, a mobile phone equipped with a fingerprint authentication function, 2003. [Online; accessed February 20, 2018].

[44] M. Gao, X. Hu, B. Cao, and D. Li. Fingerprint sensors in mobile devices. In *2014 9th IEEE Conference on Industrial Electronics and Applications*, pages 1437–1440, June 2014.

[45] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. NDSS, 2017.

[46] Walter Greenleaf. How vr technology will transform healthcare. In *ACM SIGGRAPH 2016 VR Village*, page 5. ACM, 2016.

[47] GSMARENA,Motorola ATRIX. The motorola atrix 4g, fingerprint scanner, 2011. [Online; accessed February 20, 2018].

[48] S M Taiabul Haque, Matthew Wright, and Shannon Scielzo. Passwords and interfaces: Towards creating stronger passwords by using mobile phone handsets. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones, Mobile Devices*, SPSM '13, pages 105–110, New York, NY, USA, 2013. ACM.

[49] Marian Harbach, Alexander De Luca, and Serge Egelman. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4806–4817, New York, NY, USA, 2016. ACM.

[50] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 213–230, Menlo Park, CA, 2014. USENIX Association.

[51] https://www.gettyimages.ie/. Photography depot. Technical report, [Accessed 22-Jan-2018], 2018.

[52] https://www.gsmarena.com/. Mobile phone depot. Technical report, [Accessed 22-Jan-2018], 2018.

[53] Philip G. Inglesant and M. Angela Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 383–392, New York, NY, USA, 2010. ACM.

[54] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

[55] E. A. Keshner, J. C. Slaboda, R. Buddharaju, L. Lanaria, and J. Norman. Augmenting sensory-motor conflict promotes adaptation of postural behaviors in a virtual environment. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 1379–1382, Aug 2011.

[56] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '16, pages 2156–2164, New York, NY, USA, 2016. ACM.

[57] M. H. Khan, M. S. Farid, and M. Grzegorzek. Person identification using spatiotemporal motion characteristics. In *2017 IEEE International Conference on Image Processing (ICIP)*, pages 166–170, Sept 2017.

[58] Hyoungshick Kim and Jun Ho Huh. Pin selection policies: Are they really effective? *Comput. Secur.*, 31(4):484–496, June 2012.

[59] S. K. A. Kork, I. Gowthami, X. Savatier, T. Beyrouthy, J. A. Korbane, and S. Roshdi. Biometric database for human gait recognition using wearable sensors and a smartphone. In *2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART)*, pages 1–4, Aug 2017.

[60] G. Kovelamudi, J. Zheng, and S. Mukkamala. Scramble or not, that is the question a study of the security and usability of scramble keypad for PIN unlock on smartphones. In *2016 IEEE/CIC International Conference on Communications in China (ICCC)*, pages 1–6, July 2016.

[61] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 13–19, New York, NY, USA, 2007. ACM.

[62] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. Task-driven biometric authentication of users in virtual reality (vr) environments. In Ioannis Kompatsiaris, Benoit Huet, Vasileios Mezaris, Cathal Gurrin, Wen-Huang Cheng, and Stefanos Vrochidis, editors, *MultiMedia Modeling*, pages 55–67, Cham, 2019. Springer International Publishing.

[63] Taekyoung Kwon and Sarang Na. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42:137 – 150, 2014.

[64] A. Laghari, Waheed ur Rehman, and Z. A. Memon. Biometric authentication technique using smartphone sensor. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pages 381–384, Jan 2016.

[65] LeapMotion. Leapmotion hand tracking system, 2019. [Online; accessed May 24, 2019].

[66] Lenovo's Mirage Solo. Mirage solo with daydream standalone vr headset, 2018. [Online; accessed May 7, 2018].

[67] LG Nexus 5X. Lg nexus 5x, 2019. [Online; accessed May 24, 2019].

[68] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, and Macro Gruteser. Demo of headbanger: Authenticating smart wearable devices using unique head movement patterns. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–3. IEEE, 2016.

[69] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, and Macro Gruteser. Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns. In *2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 1–9. IEEE, 2016.

[70] H. Liang, C. Fleming, and W. Wang. User authentication interfaces in mobile devices: Some design considerations. In *2014 IEEE 17th International Conference on Computational Science and Engineering*, pages 754–757, Dec 2014.

[71] Hai-Ning Liang, Charles Fleming, and Wei Wang. User Authentication Interfaces in Mobile Devices: Some Design Considerations. In *2014 IEEE 17th International Conference on Computational Science and Engineering*, pages 754–757, Chengdu, China, December 2014. IEEE.

[72] Hong Lu, Jonathan Huang, Tanwistha Saha, and Lama Nachman. Unobtrusive gait verification for mobile phones. In *Proceedings of the 2014 ACM international symposium on wearable computers*, pages 91–98. ACM, 2014.

[73] S. Mann, M. L. Hao, M. Tsai, M. Hafezi, A. Azad, and F. Keramatimoezabad. Effectiveness of integral kinesiology feedback for fitness-based games. In *2018 IEEE Games, Entertainment, Media Conference (GEM)*, pages 1–9, Aug 2018.

[74] Andrea H. Mason, Masuma A. Walji, Elaine J. Lee, and Christine L. MacKenzie. Reaching movements to augmented and graphic objects in virtual environments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI01, page 426–433. Association for Computing Machinery, 2001.

[75] S. V. Maydebura, D. H. Jeong, and B. Yu. Understanding environmental influences on performing password-based mobile authentication. In *2013 IEEE 14th International Conference on Information Reuse Integration (IRI)*, pages 728–731, Aug 2013.

[76] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 173–186, New York, NY, USA, 2013. ACM.

[77] Media Video Games and Gaming. Virtual reality (vr) and augmented reality (ar) device ownership and purchase intent among consumers in the united states as of 1st quarter 2017, by age group, 2018. [Online; accessed February 28, 2020].

[78] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L.

Mazurek. Usability and security of text passwords on mobile devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 527–539, New York, NY, USA, 2016. ACM.

[79] Arik Messerman, Tarik Mustafić, Seyit Ahmet Camtepe, and Sahin Albayrak. Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In *2011 International Joint Conference on Biometrics (IJCB)*, pages 1–8. IEEE, 2011.

[80] Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, and Hilmi Güneş Kayacik. Why aren't users using protection? investigating the usability of smartphone locking. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, pages 284–294, New York, NY, USA, 2015. ACM.

[81] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. Real-time continuous iris recognition for authentication using an eye tracker. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 1007–1009. ACM, 2012.

[82] R. Molva, D. Samfat, and G. Tsudik. Authentication of mobile users. *IEEE Network*, 8(2):26–34, March 1994.

[83] Fabian Monrose, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, 2002.

[84] Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. In *Proceedings of the 5th USENIX Conference on Offensive Technologies*, WOOT'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[85] MS HoloLens. Microsoft hololens, 2018. [Online; accessed May 4, 2018].

[86] F. Muheidat and H. W. Tyrer. Deriving information from low spatial resolution floor-based personnel detection system. In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 251–252, July 2017.

[87] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. Unsure how to authenticate on your vr headset? come on, use your head! In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, CODASPY, page 23–30. Association for Computing Machinery, 2018.

[88] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. Unsure how to authenticate on your vr headset?: Come on, use your head! pages 23–30, 03 2018.

[89] Isao Nakanishi, Sadanao Baba, and Chisei Miyamoto. Eeg based biometric authentication using new spectral features. In *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pages 651–654. IEEE, 2009.

[90] Alexander Ng. The effects of encumbrance on mobile interactions. In *Proceedings of the 16th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '14, pages 405–406, New York, NY, USA, 2014. ACM.

[91] Alexander Ng and Stephen Brewster. The relationship between encumbrance and walking speed on mobile interactions. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '13, pages 1359–1364, New York, NY, USA, 2013. ACM.

[92] Alexander Ng, Stephen A. Brewster, and John H. Williamson. Investigating the effects of encumbrance on one- and two- handed interactions with mobile devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 1981–1990, New York, NY, USA, 2014. ACM.

[93] Alexander Ng, Stephen A. Brewster, and John H. Williamson. Investigating the effects of encumbrance on one- and two- handed interactions with mobile devices. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 1981–1990, New York, NY, USA, 2014. ACM.

[94] Alexander Ng, John Williamson, and Stephen Brewster. The Effects of Encumbrance and Mobility on Touch-Based Gesture Interactions for Mobile Phones. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile*

Devices and Services - MobileHCI '15, pages 536–546, Copenhagen, Denmark, 2015. ACM Press.

[95] Alexander Ng, John Williamson, and Stephen Brewster. The effects of encumbrance and mobility on touch-based gesture interactions for mobile phones. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, pages 536–546, New York, NY, USA, 2015. ACM.

[96] Alexander Ng, John H. Williamson, and Stephen A. Brewster. Comparing evaluation methods for encumbrance and walking on interaction with touchscreen mobile devices. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services - MobileHCI '14*, pages 23–32, Toronto, ON, Canada, 2014. ACM Press.

[97] Ba Linh Nguyen, Youssef Chahir, Michèle Molina, Charles Tijus, and François Jouen. Eye gaze tracking with free head movements using a single camera. In *Proceedings of the 2010 Symposium on Information and Communication Technology*, SoICT '10, pages 108–113, New York, NY, USA, 2010. ACM.

[98] Nokia 9000 Communicator. The nokia 9000 communicator, 2018. [Online; accessed March 6th, 2018].

[99] Oculus VR. Oculus go, 2018. [Online; accessed May 4, 2018].

[100] Mcchester Odoh and Ihedigbo Chinedum E. Implementing 3d graphical password schemes. volume 9 of *6*, pages 2009–17. IOSR Journal of Electronics and Communication Engineering, 2014.

[101] Takehiko Ohno, Naoki Mukawa, and Atsushi Yoshikawa. Freegaze: A gaze tracking system for everyday gaze interaction. In *Proceedings of the 2002 Symposium on Eye Tracking Research & Applications*, ETRA '02, pages 125–132, New York, NY, USA, 2002. ACM.

[102] I. Olade, H. Liang, and C. Fleming. A review of multimodal facial biometric authentication methods in mobile devices and their application in head mounted displays. In *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet*

of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pages 1997–2004, Oct 2018.

[103] Ilesanmi Olade, Hai-ning Liang, and Charles Fleming. A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 1997–2004, Guangzhou, China, October 2018. IEEE.

[104] OPEN VR SDL API. Openvr sdk and api by valve for steamvr, 2018. [Online; accessed November 11, 2018].

[105] OptiTrack. Optitrack - motion capture systems, 2018. [Online; accessed March 6th, 2018].

[106] OSVR VR Gaming API. Osvr - open-source virtual reality for gaming, 2018. [Online; accessed November 19, 2018].

[107] Pekka Parhi, Amy K. Karlson, and Benjamin B. Bederson. Target size study for one-handed thumb use on small touchscreen devices. In *Proceedings of the 8th Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '06, pages 203–210, New York, NY, USA, 2006. ACM.

[108] Passfaces. Passfaces: Two factor authentication for the enterprise, 2018. [Online; accessed March 27, 2018].

[109] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 110:1–110:12, New York, NY, USA, 2019. ACM.

[110] Jartuwat Rajruangrabin and Dan O. Popa. Realistic and robust head-eye coordination of conversational robot actors in human tracking applications. In *Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments*, PETRA 9, page 1–7. Association for Computing Machinery, 2009.

[111] I. Rallis, A. Langis, I. Georgoulas, A. Voulodimos, N. Doulamis, and A. Doulamis. An embodied learning game using kinect and labanotation for analysis and visualization of dance kinesiology. In *2018 10th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games)*, pages 1–8, Sep. 2018.

[112] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. User verification leveraging gait recognition for smartphone enabled mobile healthcare systems. *IEEE Transactions on Mobile Computing*, 14(9):1961–1974, Sept 2015.

[113] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. Progressive authentication: Deciding when to authenticate on mobile phones. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, pages 15–15, Berkeley, CA, USA, 2012. USENIX Association.

[114] Cynthia E Rogers, Alexander W Witt, Alexander D Solomon, and Krishna K Venkatasubramanian. An approach for user identification for head-mounted displays. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers*, pages 143–146. ACM, 2015.

[115] Joseph Roth, Xiaoming Liu, and Dimitris Metaxas. On continuous user authentication via typing behavior. *IEEE Transactions on Image Processing*, 23(10):4611–4624, 2014.

[116] U. Saeed, F. Matta, and J. Dugelay. Person recognition based on head and mouth dynamics. In *2006 IEEE Workshop on Multimedia Signal Processing*, pages 29–32, Oct 2006.

[117] S Sangani, J Fung, R Kizony, ST Koenig, and PL Weiss. Navigating and shopping in a complex virtual urban mall to evaluate cognitive functions. In *2013 International Conference on Virtual Rehabilitation (ICVR)*, pages 9–14. IEEE, 2013.

[118] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 11:1–11:14, New York, NY, USA, 2013. ACM.

[119] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In

Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pages 1379–1384. ACM, 2016.

[120] Abdul Serwadda, Vir V Phoha, Sujit Poudel, Leanne M Hirshfield, Danushka Bandara, Sarah E Bratt, and Mark R Costa. fnirs: A new modality for brain activity-based biometric authentication. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–7. IEEE, 2015.

[121] Abdul Serwadda, Vir V Phoha, and Zibo Wang. Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2013.

[122] C. E. Shannon. A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(1):3–55, January 2001.

[123] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 2:1–2:20, New York, NY, USA, 2010. ACM.

[124] Y. Shen, H. Wen, C. Luo, W. Xu, T. Zhang, W. Hu, and D. Rus. Gaitlock: Protect virtual and augmented reality headsets using gait. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2018.

[125] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. Using reflexive eye movements for fast challenge-response authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1056–1067, New York, NY, USA, 2016. ACM.

[126] Craig Stewart, Eve Hoggan, Laura Haverinen, Hugues Salamin, and Giulio Jacucci. An exploration of inadvertent variations in mobile pressure input. In *Proceedings of the 14th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '12, pages 35–38, New York, NY, USA, 2012. ACM.

[127] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 15:1–15:14, New York, NY, USA, 2013. ACM.

[128] Mohammad Tamviruzzaman, Sheikh Iqbal Ahamed, Chowdhury Sharif Hasan, and Casey O'brien. epet: when cellular phone learns to recognize its owner. In *Proceedings of the 2nd ACM workshop on Assurable and usable security configuration*, pages 13–18. ACM, 2009.

[129] Hai Tao and Carlisle M. Adams. Pass-go: A proposal to improve the usability of graphical passwords. *I. J. Network Security*, 7:273–292, 2008.

[130] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, pages 56–66, New York, NY, USA, 2006. ACM.

[131] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. A survey on touch dynamics authentication in mobile devices. *Computers & Security*, 59:210 – 235, 2016.

[132] Tobii Pro VR Integration. Tobii pro vr integration based on htc vive hmd, 2018. [Online; accessed May 4, 2018].

[133] Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha, and Ketan Vyas. Pass-o: A proposal to improve the security of pattern unlock scheme. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, pages 400–407, New York, NY, USA, 2017. ACM.

[134] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, CCS '13, pages 161–172, New York, NY, USA, 2013. ACM.

[135] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How does your password measure up? the effect of strength meters on password creation. In *Proceedings of the 21st USENIX*

Conference on Security Symposium, Security'12, pages 5–5, Berkeley, CA, USA, 2012. USENIX Association.

[136] J. Vaughan, P. M. Green, M. Salter, B. Grieve, and K. B. Ozanyan. Floor sensors of animal weight and gait for precision livestock farming. In *2017 IEEE SENSORS*, pages 1–3, Oct 2017.

[137] VIVE Virtual Reality System. Vive^{TM} — vive virtual reality system, 2018. [Online; accessed May 24, 2019].

[138] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1403–1406, New York, NY, USA, 2015. ACM.

[139] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, NordiCHI '14, pages 461–470, New York, NY, USA, 2014. ACM.

[140] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 261–270, New York, NY, USA, 2013. ACM.

[141] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces*, IUI '13, pages 277–286, New York, NY, USA, 2013. ACM.

[142] Yanqing Wang, Christine L. MacKenzie, Valerie A. Summers, and Kellogg S. Booth. The structure of object transportation and orientation in human-computer interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI98, page 312–319. Association for Computing Machinery, 1998.

[143] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 162–175, New York, NY, USA, 2010. ACM.

[144] Roman Weiss and Alexander De Luca. Passshapes: Utilizing stroke based authentication to increase password memorability. In *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*, NordiCHI '08, pages 383–392, New York, NY, USA, 2008. ACM.

[145] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 1–12, New York, NY, USA, 2005. ACM.

[146] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1):102 – 127, 2005. HCI research in privacy and security.

[147] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, July 2005.

[148] Dhruv Kumar Yadav, Beatrice Ionascu, Sai Vamsi Krishna Ongole, Aditi Roy, and Nasir Memon. Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass. In *International conference on financial cryptography and data security*, pages 281–297. Springer, 2015.

[149] Shanhe Yi, Zhengrui Qin, Ed Novak, Yafeng Yin, and Qun Li. Glassgesture: Exploring head gesture interface of smart glasses. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9. IEEE, 2016.

[150] Z. Yu, H. Liang, C. Fleming, and K. L. Man. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pages 458–460, Oct 2016.

[151] Z. Yu, I. Olade, H. N. Liang, and C. Fleming. Usable authentication mechanisms for mobile devices: An exploration of 3d graphical passwords. In *2016 International Conference on Platform Technology and Service (PlatCon)*, pages 1–3, Feb 2016.

[152] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 6:1–6:12, New York, NY, USA, 2011. ACM.

Declaration of Authorship

I, **ILESANMI AYODEJI OLADE**, declare that this thesis titled,**"Usable Secure Interfaces for Mobile Devices"** and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

_____

Date:

_____